

SysTechDev 2026

INTERNATIONAL CONFERENCE ON SECURE SYSTEMS
DESIGN AND TECHNOLOGY DEVELOPMENT

NATIONAL MILITARY UNIVERSITY "VASIL LEVSKI"

ESTONIAN UNIVERSITY OF LIFE SCIENCES

VIDZEME UNIVERSITY OF APPLIED SCIENCES

GREEN FUTURE TECHNOLOGIES

SECURE SYSTEMS DESIGN AND TECHNOLOGY DEVELOPMENT (SysTechDev)

International Conference Proceedings

25-26 June 2026

VOLUME I



Veliko Tarnovo, Bulgaria 2026

NATIONAL MILITARY UNIVERSITY "VASIL LEVSKI"

ESTONIAN UNIVERSITY OF LIFE SCIENCES

VIDZEME UNIVERSITY OF APPLIED SCIENCES

GREEN FUTURE TECHNOLOGIES

Proceedings of the International Conference
**Secure Systems Design and Technology
Development (SysTechDev)**
25–26 June 2026

Volume I

Veliko Tarnovo, Bulgaria
2026

Secure Systems Design and Technology Development (SysTechDev). Proceedings of the 1st International Scientific Conference, June 25–26, 2026. *Volume I.* National Military University "Vasil Levski", Veliko Tarnovo, Bulgaria, 2026. 523 pp.

The three-volume proceedings of the 1st International Scientific Conference "Secure Systems Design and Technology Development (SysTechDev)" present the latest research in defense and security technologies, engineering sciences and production technologies, information technologies, sustainable energy engineering and applications, laser technologies, materials science, mechanics, metalworking, mathematical modelling, and electrical engineering.

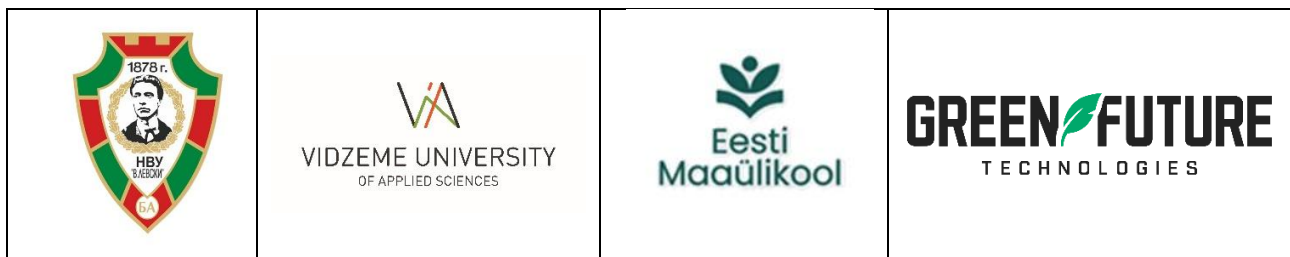
The conference is interdisciplinary, bringing together the achievements of international research teams. The scope of the studies presented in these proceedings is broad and multidisciplinary, reflecting the results of collaborative research conducted by scientists from different countries.

The conference proceedings include 196 scientific papers, with participants representing 16 countries.

The 1st International Scientific and Practical Conference on Secure Systems Design and Technology Development (SysTechDev) took place at the National Military University "Vasil Levski" in Veliko Tarnovo, Bulgaria, on June 25–26, 2026.

<https://etrconf.eu/>

Link to conference proceedings: <https://journal.etrconf.eu/std/issue/archive>



This journal is licensed under
[Creative Commons Attribution 4.0 International \(CC BY 4.0\) License](https://creativecommons.org/licenses/by/4.0/)
The author of the paper takes responsibility for the content of the paper



Online ISSN 3044-7771

Published by Green Future Technologies SIA, 2026

Scientific Committee Co-Chairman

Dr.sc.ing. Lyubomir Lazov, Rezekne Academy of Riga Technical University, Latvia
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
Dr.sc.ing. Artis Teilāns, Vidzeme University of Applied Sciences, Latvia

Scientific Committee

PhD Sherif Ibrahim Abdel-Wahab, Agricultural Research Center, Giza, Egypt
PhD prof. Tamer Ibrahim Abdel-Wahab, Agricultural Research Center, Giza, Egypt
PhD prof. Hikmat Almadhkhori, Al-Mustansiriyah University, Baghdad, Iraq
PhD Nikolaj Angelov, Technical University of Gabrovo, Bulgaria
PhD Kiril Anguelov, Technical University of Sofia, Bulgaria
PhD Andres Annuk, Estonian University of Life Sciences, Estonia
PhD Ekaterina Arabska, Higher School of Agribusiness and Regional Development, Bulgaria
PhD Wael Badawy, International Atomic Energy Agency, Egypt
PhD Stefan Bankov, The Ministry of Interior of Bulgaria, Bulgaria
PhD Plamen Bogdanov, University of Library Studies and Information Technologies, Bulgaria
PhD Hamid Can, Trakya University, Turkey
PhD Arnis Cīrulis, Vidzeme University of Applied Sciences, Latvia
PhD Dimitar Dimitrov, Todor Kableskov University of Transport, Bulgaria
PhD Nadezhda Dimova, New Bulgarian University, Bulgaria
PhD Tamar Dolbaia, Tbilisi State University, Georgia
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
PhD Nino Durglishvili, Tbilisi State University, Georgia
Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia
Dr.sc.ing. Pēteris Grabusts, Rezekne Academy of Riga Technical University, Latvia
PhD Gilbert-Rainer Gillich, University Babes-Bolyai, Romania
PhD Grigor Grigorov, "Vasil Levski" National Military University, Bulgaria
PhD Mariusz Gontarczyk, Military University of Technology, Poland
PhD Tzvetelin Gueorguiev, Technical University of Gabrovo, Bulgaria
PhD Alexandru Herciu, „CAROL I” National Defense University, Romania
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
PhD Valery Ivanov, Defense Institute "Professor Tsvetan Lazarov", Bulgaria
DSc Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria
Dr.sc.ing. Aivars Kaķītis, Latvia University of Life Sciences and Technologies, Latvia
PhD Georgi Kamarashev, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria
Dr.paed. Ilmārs Kangro, Rezekne Academy of Riga Technical University, Latvia
PhD Atis Kapenieks, Riga Technical University, Latvia
Dr. paed. Janis Kapenieks, Riga Technical University, Latvia
PhD Stancho Kajkov, "Vasil Levski" National Military University, Bulgaria
PhD Anna Khilya, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Spain
PhD Noah Ugur Kilinc, Piri Reis University, Istanbul, Turkey
PhD Georgi Komitov, Agricultural University Plovdiv, Bulgaria
PhD Lazar Lazarov, "Vasil Levski" National Military University, Bulgaria
Dr.sc.ing. Lyubomir Lazov, Rezekne Academy of Riga Technical University, Latvia
PhD Lyuboslav Lyubenov, University of Ruse "Angel Kanchev", Bulgaria

PhD Wilmer Orlando López González, Universidad Nacional de Educación, Ecuador
 PhD Tatyana Maglyovana, National University of Civil Protection of Ukraine, Ukraine
 Dr.sc.math. Maksims Marinaki, University of Latvia, Latvia
 PhD Rumen Marinov, "Vasil Levski" National Military University, Bulgaria
 PhD Georgi Marinov, Rakovski National Defence College, Bulgaria
 PhD Dilyan Markov, Georgi Rakovski Military Academy, Bulgaria
 PhD Otakar Jiří Mika, Police Academy and South Bohemian University, Czech Republic
 PhD Gregg Tyler Milligan, University of Canton, United States
 PhD Cristian Emil Moldoveanu, Military Technical Academy "Ferdinand I", Romania
 Dr.sc.ing. Marufjon Musaeu, Tashkent State Technical University, Uzbekistan
 PhD Serhii Naida, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
 PhD Nikolay Nichev, Georgi Benkovski Higher Military Air School, Bulgaria
 PhD Plamen Pavlov, School of Telecommunications and Posts, Bulgaria
 Dr.sc.ing. Desislava Petrova, Technical University of Gabrovo, Bulgaria
 PhD Dimcho Pulov, Technical University of Gabrovo, Bulgaria
 PhD Prof. Vesela Radovic, University of Belgrade, Serbia
 PhD Tomas Rozsypal, University of Defence, Czech Republic
 PhD Rashmi Jaymin-Sanchaniya, Riga Technical University, Latvia
 PhD Yehya A. Salih, Head of Department at University of Basrah, Iraq
 PhD Iryna Sarancha, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Ukraine
 PhD Barbara Sawicka, University of Life Sciences in Lublin, Poland
 PhD Dafinka Sidova, New Bulgarian University, Bulgaria
 Dr.sc.ing. Andris Skromulis, Rezekne Academy of Riga Technical University, Latvia
 Dr.sc.ing. Adiljan Suleymanov, Tashkent State Technical University, Uzbekistan
 Dr.-Ing. Bambang Soemardiono, Institut Teknologi Sepuluh Nopember, Indonesia
 Dr.sc.ing. Artis Teilāns, Vidzeme University of Applied Sciences, Latvia
 PhD Ērika Teirumnieka, Rezekne Academy of Riga Technical University, Latvia
 Dr.biol. Rasma Tretjakova, Rezekne Academy of Riga Technical University, Latvia
 PhD Antonios Valamontes, Research Director at Kapodistrian Academy of Science, United States
 PhD Sergij Vambol, National Technical University, Kharkiv Polytechnic Institute, Ukraine
 PhD Viola Vambol, University of Yuri Kondratyuk Poltava Polytechnic National University, Ukraine
 PhD Valentin Vassilev, New Bulgarian University, Bulgaria
 PhD Algazy Zhauyt, Almaty University of Power Engineering and Telecommunications, Kazakhstan
 Dr.sc.ing. Inga Zinicovscaia, Horia Hulubei National Institute for Physics and Nuclear Engineering, Romania

Organising Committee Chairman

PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria

Organising Committee

Aigars Abrickis, Green Future Technologies Ltd., Latvia
 MA Yanitsa Boyanova, "Vasil Levski" National Military University, Bulgaria
 Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia
 Dr.sc.ing. Pēteris Grabusts, Rezekne Academy of Riga Technical University, Latvia
 MA Georgi Hristov, "Vasil Levski" National Military University, Bulgaria
 PhD Ērika Teirumnieka, Rezekne Academy of Riga Technical University, Latvia
 MA Svetoslav Pashunov, "Vasil Levski" National Military University, Bulgaria

Reviewers

PhD Andres Annuk - Estonian University of Life Sciences, Estonia
PhD Dimitar Angelski, Forestry Technical University, Bulgaria
PhD Svilena Arabadzhieva, Academy of the Ministry of Interior, Bulgaria
PhD Plamen Atanasov, New Bulgarian University, Bulgaria
PhD Stefan Bankov, The Ministry of Interior of Bulgaria, Bulgaria
PhD Daniel Berchev, "Vasil Levski" National Military University, Bulgaria
PhD Rosen Bogdanov, "Vasil Levski" National Military University, Bulgaria
PhD Olga Borisova, Varna Free University Chernorizets Hrabar, Bulgaria
PhD Erol Buyukliev, Rakovski National Defence College, Bulgaria
PhD Arnis Cīrulis, Vidzeme University of Applied Sciences, Latvia
PhD Aija Cunska, Vidzeme University of Applied Sciences, Latvia
PhD Iveta Daugule, University of Latvia, Latvia
PhD Dilyana Dimitrova, Nikola Vaptsarov Naval Academy, Bulgaria
PhD Desislava Dimitrova, Technical University of Varna, Bulgaria
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
PhD Kliment Georgiev, Technical University of Sofia, branch Plovdiv, Bulgaria
PhD Pēteris Grabusts, Riga Technical University, Latvia
PhD Aleksandrs Gorbunovs, Riga Technical University, Latvia
PhD Iliayn Hutov, Defense Institute "Professor Tsvetan Lazarov", Bulgaria
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
PhD Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo", Bulgaria
PhD Martins Jansevskis, Vidzeme University of Applied Sciences, Latvia
PhD Oskars Java, Vidzeme University of Applied Sciences, Latvia
PhD Sandra Kaija, Riga Stradiņš University, Latvia
PhD Ilmārs Kangro, Rezekne Academy of Riga Technical University, Latvia
PhD Atis Kapenieks, Riga Technical University, Latvia
PhD Kiril Lengerov, TU Sofia, branch Plovdiv, Bulgaria
PhD Lyuboslav Lyubenov, University of Ruse "Angel Kanchev", Bulgaria
PhD Dilyan Markov, Georgi Rakovski Military Academy, Bulgaria
PhD Ventsislava Nikolova-Minkova, Technical University of Gabrovo, Bulgaria
PhD Daniela Pavlova, University of Library Studies and Information Technologies, Bulgaria
PhD Nikolay Padarev, "Vasil Levski" National Military University, Bulgaria
PhD Penyo Penev, "Georgi Benkovski" Bulgarian Air Force Academy, Bulgaria
PhD Desislava Petrova, Technical University of Gabrovo, Bulgaria
PhD Dimcho Pulov, Technical University of Gabrovo, Bulgaria
PhD Hristo Radev, Technical University of Gabrovo, Bulgaria
PhD Zhaneta Savova, National Military University, Bulgaria
PhD Dafinka Sidova, New Bulgarian University, Bulgaria
PhD Krasimir Slavyanov, "Vasil Levski" National Military University, Bulgaria
PhD Milko Stefanov, Rakovski National Defense College, Bulgaria
PhD Ivan Tashev, Technical University Sofia, branch Plovdiv, Bulgaria
PhD Artis Teilāns, Vidzeme University of Applied Sciences, Latvia
PhD Tsvetoslav Tsankov, Konstantin Preslavsky University of Shumen, Bulgaria
PhD Kostadin Trifonov, University of Transport Todor Kableshev, Bulgaria
PhD Valentin Vassilev, South-West University "Neofit Rilski", Bulgaria
PhD Stoyan Vergiev, Technical University of Varna, Bulgaria
PhD Beata Vlahova, National Military University Vasil Levski, Bulgaria
PhD Emil Yankov, University of Ruse, Bulgaria
PhD Tsanka Zlateva-Petkova, Technical University of Gabrovo, Bulgaria

Volume I

CONTENTS

Defence and Security Technology

Kiril Anguelov, Philip Stoyanov CORPORATE RESPONSIBILITY IN SUSTAINABLE SUPPLY CHAINS: EXTENDED ROLES AND IMPLICATIONS	15-21
Kiril Anguelov, Philip Stoyanov, Rima Tamošiūnienė CSR AND EMPLOYEE WELL-BEING IN SUSTAINABLE HUMAN RESOURCE MANAGEMENT	23-29
Kiril Anguelov, Miglena Angelova ALGORITHMIC MANAGEMENT AS A DRIVER OF ACCELERATED GROWTH IN HIGH-GROWTH FIRMS	31-36
Svilena Arabadzhieva INTERNAL FIRE HYDRANTS IN RESIDENTIAL AND PUBLIC BUILDINGS AS A FIRE-RISK MITIGATION MEASURE	37-42
Plamen Atanasov TWO APPROACHES TO SEEKING PUBLIC SUPPORT IN ADDRESSING CHALLENGES IN THE FIELD OF INTERNATIONAL SECURITY	43-50
Plamen Atanasov, Evelina Atanasova THE HYBRID WARFARE IN CYBERSPACE	51-56
Nevena Atanasova-Krasteva CHALLENGES AND ACHIEVEMENTS IN THE EDUCATION IN THE GENDER PERSPECTIVES IN SECURITY AND DEFENSE'S COMMON MODULE	57-63
Daniel Berchev, Monika Panayotova THE CRISIS AROUND GREENLAND AND THE TEST FOR NATO AND THE EUROPEAN UNION: LEGAL LIMITS OF TERRITORIAL CLAIMS AND TOOLS AGAINST COERCION	65-76
Daniel Berchev COMPARATIVE ANALYSIS OF THE NATIONAL SECURITY STRATEGIES OF BULGARIA, THE USA, RUSSIA AND CHINA THROUGH THE PRISM OF KEY SECURITY THEORIES	77-86
Yanitsa Boyanova RADIOGENIC HEAT PRODUCTION IN THE EARTH'S CRUST OF BULGARIA: THE DOMINANT ROLE OF THE RHODOPE MASSIF	87-91
Stefko Burdzhiev, Georgi Georgiev ENVIRONMENTAL, SANITARY AND HEALTH REQUIREMENTS IN THE DESIGN AND OPERATION OF RADIATION-HAZARDOUS FACILITIES	93-100

Georgi Dimitrov MEDIATION AS A RISK MANAGEMENT INSTRUMENT REFRAMING ORGANIZATIONAL CONFLICT AS A MISSING STRUCTURAL ELEMENT IN ERM FRAMEWORKS	101-107
Vihra Dimitrova INTEGRATION OF DIGITAL AND ARTIFICIAL INTELLIGENCE SOLUTIONS IN MENTAL HEALTHCARE	109-116
Desislava Dimitrova, Daniela Toneva WATER RESOURCES EXPLOITATION IN BULGARIA: A WATER SECURITY PERSPECTIVE	117-122
Ekaterina Dyankova, Dilyana Dimitrova AN INTEGRATED SIMULATION MODEL FOR MARITIME CYBERSECURITY: A COMPARATIVE RESEARCH ANALYSIS APPROACH	123-129
Ekaterina Dyankova, Dilyana Dimitrova, Evgeni Andreev DESIGN AND SCENARIO DEVELOPMENT OF A MARITIME CYBERSECURITY TRAINING SIMULATION PLATFORM	131-139
Nikolay Dolchinkov ENERGY SECURITY AS AN ELEMENT OF NATIONAL SECURITY	141-148
Nikolay Dolchinkov RESEARCH ON THE EFFECTS OF SPECIFIC RADIONUCLIDES ON HEALTH	149-156
Nikolay Dolchinkov USE OF MOBILE AUTONOMOUS SYSTEMS TO CONTROL POLLUTION OF CONTINENTAL WATER BODIES	157-162
Nikolay Dolchinkov, Zilola Mirsharipova, Malikahon Aripadzhayeva ORGANIZING AND CONDUCTING UNDERWATER SEARCH AND RESCUE OPERATIONS FOR VICTIMS	163-168
Angel Genchev, Emil Ivanov EXPECTATIONS AND OPPORTUNITIES FOR AI-ENABLED SYSTEMS APPLICATION IN THE CONTEXT OF MILITARY COMMUNICATIONS AND CYBERSECURITY	169-173
Georgi Georgiev, Stefko Burdzhiev AN INTEGRATED CONCEPT FOR THE PROTECTION OF PHOTOGRAPHIC AND ELECTRONIC EQUIPMENT DURING CRIME SCENE INVESTIGATION USING A RISK-ORIENTED PROTOCOL	175-182
Teodora Georgieva, Ivo Radulov LEADERSHIP EXPECTATIONS ACROSS STRATEGIC, OPERATIONAL, AND TACTICAL C2 LEVELS IN A HYPOTHETICAL MILITARY OPERATION: THE INFLUENCE OF PROCEDURAL JUSTICE, TRUST IN LEADERS, AND DIGITALIZATION IN PEACETIME SETTINGS	183-190
Genadiy Gospodinov, Tamara Ristovska, Tito Titov, Kiril Nikolov, Andriyan Stoilov, Kliment Toshkov LIGHTWEIGHT COMPARATIVE EVALUATION OF QUANTUM AND HYBRID QUANTUM- CLASSICAL MACHINE LEARNING MODELS FOR INTRUSION DETECTION	191-197

Teodora Grozdanova COMPARATIVE ANALYSIS OF MOTIVATIONAL FACTORS FOR SERVICE IN THE BULGARIAN ARMED FORCES (2017–2025)	199-202
Viktor Hristov, Miglena Angelova AI-DRIVEN MODEL FOR ECONOMIC EFFICIENCY IN SOFTWARE DEVELOPMENT TASKS	203-208
Iliyan Hutoy, Dilyan Nedelchev CONDITION BASED AND RISK ORIENTED LIFECYCLE SAFETY MANAGEMENT OF CONVENTIONAL AMMUNITION USING NON-DESTRUCTIVE DIAGNOSTIC DATA	209-214
Iliyan Hutoy, Ivan Ivanov, Hristo Hristov AI-ENABLED MULTI-SENSOR FUSION FOR FIELD DETECTION OF CHEMICAL WARFARE AGENTS: A SYSTEM-ORIENTED EXPERIMENTAL STUDY	215-221
Emil Ivanov RISKS AND MITIGATION MEASURES IN THE INTEGRATION OF ARTIFICIAL INTELLIGENCE INTO THE COMMAND CHAINS OF THE ARMED FORCES	223-228
Valeri Ivanov, Kristiyan Petrov PSYCHOLOGICAL QUALITIES OF STRATEGIC LEADERS AND THEIR SIGNIFICANCE FOR PROFESSIONAL SELECTION IN THE NATIONAL SECURITY SYSTEM	229-232
Ivan Ivanov, Sevdalin Spasov ELECTROMAGNETIC PROTECTION USING SOFTWARE-DEFINED RADIO	233-240
Alexander Yankov ASSESSMENT OF EU DIGITAL IDENTITY WALLET FROM SECURITY PERSPECTIVE	241-245
Lyuboslav Lyubenov CRIMINALIZATION AS A TOOL FOR ENSURING NATIONAL SECURITY IN THE MODERN RULE OF LAW. (SHORT LOGICAL STATEMENT)	247-251
Kiril Luchkov, Mihail Chipriyanov, Galina Chipriyanova, Nadezhda Veselinova, Tihomir Panov INTEGRATING GREEN BUILDING INTO NATIONAL DEFENSE SYSTEMS	253-259
Kiril Luchkov MANAGING ENVIRONMENTAL RISKS THROUGH ESG	261-266
Kiril Luchkov, Mihail Chipriyanov, Galina Chipriyanova CHALLENGES IN THE DEVELOPMENT OF AUTONOMOUS ENERGY MICROGRIDS IN BULGARIA	267-271
Kiril Luchkov, Mihail Chipriyanov, Galina Chipriyanova AN INTEGRATED APPROACH TO THE SECURITY OF ENERGY INFRASTRUCTURE: PROBLEMS AND INNOVATIVE SOLUTIONS	273-277
Elina Marinova FISCAL SECURITY AND NON-COMPLIANT TAX CONDUCT	279-285

Galina Mileva A COMPREHENSIVE APPROACH TO ASSESSING THE SECURITY OF BUILT HERITAGE SITES USING FIRE RISK ANALYSIS AND EVALUATION METHODOLOGY	287-296
Marufjan Musaev, Azizjon Boboev, Feruza Boboeva, Tolibjonov Otabeko'gli REDUCTION OF THE SPECIFIC ACTIVITY OF RADIOACTIVELY CONTAMINATED SOIL USING THE HIGH-PRESSURE HYDRO-CLEANING METHOD	297-301
Svilen Neykov, Rosen Iliev ANALYSIS OF THE HUMAN BODY POSITIONING IN DISASTER REMEDIATION	303-310
Atanas Nikolov ASSESSMENT OF THE APPLICABILITY OF INTERNATIONAL FRAMEWORKS AND STANDARDS FOR CYBERSECURITY AS A BASIS FOR BUILDING A CLASSIFICATION MODEL IN THE "SECURITY AND DEFENCE" SECTOR	311-319
Silvia Nikolova, Tsvetoslav Tsankov A HYBRID PROBABILISTIC AND FMEA-BASED MODEL FOR RELIABILITY AND FAULT TOLERANCE ASSESSMENT OF AI-BASED SECURITY SYSTEMS	321-327
Monika Panayotova THE KEY ROLE OF SMES IN THE EUROPEAN DEFENSE ECOSYSTEM WITH EMPHASIS ON QUANTUM TECHNOLOGIES	329-339
Vasil Pavlov, Raquel Cardoso, Panagiota (Naya) Kalfeli CLIMATE-INDUCED MIGRATION TO THE EU: LEGAL PROTECTION GAPS AND THE ROLE OF MEDIA NARRATIVES	341-349
Nikolay Penev, Daniela Pavlova, Jasen Tanev, Nikolay Koev, Andrian Stoilov, Kiril Nikolov PHYSICAL VULNERABILITY OF CYBER SYSTEMS: ANALYSIS OF INCIDENTS, RISK FACTORS AND SECURITY STRATEGIES	351-355
Elitsa Petkova A "BRUTE FORCE" REDUCED ATTACK IMPLEMENTATION ON 256 - AES ENCRYPTED VOICE STREAM IN A MATLAB SIMULINK ENVIRONMENT	357-361
Elitsa Petkova, Mario Angelov VERIFYING ASPECTS AN "BRUTE FORCE" ATTACK ON 256 - AES ENCRYPTED VOICE STREAM	363-367
Zhivo Petrov, Lyubosvet Stoev COMPACT CRITICAL INFRASTRUCTURE ACTIVE DRONE PROTECTION SYSTEM – CONCEPTUAL DESIGN	369-375
Mihai Petrov INTEGRATED STUDY OF OCEAN WARMING, CO ₂ UPTAKE, AND ACIDIFICATION UNDER ANTHROPOGENIC EMISSIONS	377-386
Mihai Petrov COMPETING THERMODYNAMIC AND RADIATIVE EFFECTS ON ATMOSPHERIC CIRCULATION IN POLLUTED ENVIRONMENTS	387-398

Irena Petrova, Kostadin Trifonov INTEGRATED RISK ASSESSMENT MODEL FOR CYBER THREATS TO CRITICAL INFRASTRUCTURE	399-407
Ivo G. Radulov A METHODOLOGY FOR STRATEGIC DEFENSE REVIEW AND ITS GOVERNANCE SYSTEM. (PROTOTYPE)	409-416
Tamara Ristovska, Lyubomir Gotsev, Genadiy Gospodinov, Jordan Deliversky, Stanislava Cholova EFFICIENT AND TRUSTWORTHY ANTI-CORRUPTION AI: LEVERAGING MODEL PRUNING FOR SECURE DEPLOYMENT IN CRITICAL SYSTEMS	417-423
Miroslava Robinson, Daniela Toneva ENVIRONMENTAL SECURITY AND MARINE ECOSYSTEM PROTECTION: ADDRESSING REGULATORY AMBIGUITIES IN BULGARIA	425-429
Sabin Sabev APPLICATION OF THE BROKEN WINDOWS THEORY IN THE CONTEXT OF MILITARY ORGANIZATIONAL BEHAVIOR AND DISCIPLINE	431-437
Sabin Sabev CULTURAL PARASITISM: THE TRANSFER OF FOREIGN CULTURAL MODELS AS A THREAT TO NATIONAL SECURITY	439-445
Dafinka Sidova, Valentin Vasilev, Petar Arabadzhyski ECO-LEADERSHIP AND GREEN HUMAN RESOURCE MANAGEMENT AS DRIVERS OF ENVIRONMENTAL SECURITY AND CRITICAL INFRASTRUCTURE RESILIENCE	447-453
Svilen Stefanov, Tihomir Yotkov, Iliyan Lilov, Vanya Dimitrova APPLICATION OF THE MONTE CARLO METHOD TO DETERMINE OF EVACUATION PARAMETERS FROM SETTLEMENTS	455-459
Tsanko Stefanov RESEARCH ON THE MICROELEMENTS OF THE MARKETING ENVIRONMENT OF ENTERPRISES FROM DIFFERENT INDUSTRIES	461-465
Tsanko Stefanov RESEARCH ON THE MACRO ELEMENTS OF THE MARKETING ENVIRONMENT OF COMPANIES BY INDUSTRY	467-472
Milko Stefanov OPERATIONAL ART AND COGNITIVE WARFARE	473-477
Milko Stefanov A CONCEPTUAL MODEL FOR RISK MANAGEMENT IN HYBRID THREATS AND COGNITIVE ATTACKS	479-485
Svilen Stefanov, Tihomir Yotkov, Iliyan Lilov, Vanya Dimitrova APPROACHES FOR MODELING OF SHOPPING MALL EVACUATION	487-492

Stoyko Stoykov, Valentin Vasilew, Gentian Koci DIGITAL SUSTAINABILITY: THE ROLE OF SMART HR TOOLS IN ACHIEVING SUSTAINABLE DEVELOPMENT GOALS (SDGS)	493- 498
Svetoslav Velkov WHY ECONOMIC SECURITY IS NATIONAL SECURITY. ECONOMIC DETERMINISM IN THE U.S. NATIONAL SECURITY STRATEGY 2025	499-504
Stoyan Vergiev VULNERABILITY ASSESSMENT OF WILD MEDICINAL AND AROMATIC PLANTS ALONG THE BULGARIAN BLACK SEA COAST USING RAPID GIS-BASED MODEL	505-510
Zarko I. Zdravkov, Ivo G. Radulov CRITICAL INFRASTRUCTURE RISK ASSESSMENT APPROACH	511-518
Viara Zhekova IMPROVING DISASTER, ACCIDENT, EMERGENCY AND CRISIS MANAGEMENT SYSTEMS IN BULGARIA	519-523

I

DEFENCE AND SECURITY TECHNOLOGY

Corporate Responsibility in Sustainable Supply Chains: Extended Roles and Implications

Kiril Anguelov

Management and Business Information Systems
Technical University of Sofia
Sofia, Bulgaria
ang@tu-sofia.bg

Philip Stoyanov

Management Department
University of National and World Economy
Sofia, Bulgaria
ph.stoyanov@unwe.bg

Abstract— The concept of extended corporate social responsibility is explored in the context of increasing demands on companies to manage not only their own activities, but also the effects along the entire supply chain. The analysis focuses on the role of organizations in ensuring sustainable practices, including compliance with social and environmental standards by suppliers and partners. The study is based on a survey conducted among 137 respondents in the period December 2025 - February 2026. Descriptive statistics and correlation analysis methods were used to process the data. The results show a moderate positive relationship between transparency and control in supply chains, as well as between the perception of CSR as an extended responsibility and the degree of integration of social and environmental criteria in supplier management. The results obtained outline both the main challenges and opportunities for organizations in implementing extended corporate social responsibility in modern supply chains.

Keywords— Corporate social responsibility; Sustainable supply chains; Responsible supply chain management; ESG.

I. INTRODUCTION

With the overall development of society and technological progress, Corporate Social Responsibility (CSR) has acquired new dimensions. In modern business conditions, CSR is no longer perceived only as a specific management practice, which is limited to internal organizational dimensions. The new field of responsibility of CSR is also transferred to supply chains, as the topic becomes increasingly important in conditions of globalization and a complicated geopolitical situation.

In this sense, companies are now also responsible for their suppliers, which turns CSR from an internal organizational practice to an externally oriented responsibility. With the expansion of the scope of CSR, the focus is actually shifting significantly towards practical implementation, and not so much only on completed sporadic activities.

The new statements are also related to the adoption of additional regulatory requirements for companies - i.e.

CSR is no longer so much a "voluntary" practice and a decision only for the management of an organization. This creates conditions for higher transparency, which in turn allows for better control.

There is a wealth of research in the scientific literature on CSR, but there is a lack of a clear understanding of the roles and effects that the new requirements of extended CSR will lead to. In this regard, this report focuses on the way in which CSR is extended and how it is integrated into the overall supplier management – from the selection of suppliers, through the method of assessment and implementation of control, while identifying the main challenges and opportunities arising from these transformations.

Literature review

Corporate social responsibility is gaining new dimensions in the real economy, including supply chains, where the interest of scientists in recent years has also understandably increased, especially in terms of new regulatory requirements and technological advances.

In this context, Camilleri [1] emphasizes that responsible supply chain management is becoming a strategic tool, thanks to which business organizations combine their purely economic goals with socially responsible practices, while at the same time being able to build a long-term competitive advantage on this basis. This means that responsible supply chain management is not only an obligation to comply with new regulatory requirements. It is rather a strategic choice that is formed under the influence of various external and internal factors.

Roy, Silvestre and Singh [2] state that the implementation of sustainable practices in supply chains is influenced simultaneously by two very important aspects - both external pressure from stakeholders and internal organizational factors. The scientists comment that in this context reactive and proactive approaches are defined, and according to them proactive approaches are more effective in achieving sustainable results. In turn, Damert, Koep,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.182>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Guenther and Morris [3] add that pressure from stakeholders has a significant impact on the implementation of socially responsible practices in supply chains, and this effect varies depending on the degree of internationalization of companies.

In this sense, sustainable supply chain management can be seen as a process of institutional transformation that manifests itself through different mechanisms and leads to diverse outcomes. Chikwana, Alinaghian and Razmdoost [4] believe that sustainable supply chain management in modern conditions cannot be viewed solely as a result of company strategies, as it carries much greater potential and significance. According to them, it is a process of institutional change, determined by the interaction between external pressures and internal organizational factors.

Along with external environmental pressures, organizations are also motivated to implement responsible practices due to the desire to build and protect their corporate reputation. Hoejmose, Roehrich and Grosvold [5] conclude that the implementation of responsible supply chain management is often motivated by the desire of organizations to protect their corporate reputation from negative public reactions. At the same time, however, they use these practices as a means of building a competitive advantage.

The real implementation of sustainable practices often faces significant constraints, especially in the context of small and medium-sized enterprises. Despite the growing pressure to implement socially responsible practices in supply chains, a number of studies highlight the existence of significant barriers, especially for small and medium-sized enterprises. The main barriers are mainly related to limited resources, short-term orientation, lack of coordination between partners and insufficient incentives to implement sustainable practices [6].

In response to these challenges and growing public expectations, the role of regulatory frameworks is increasing, which expand the scope of corporate responsibility. Both and Wilhelm [7] draw attention to the fact that modern regulations related to due diligence in supply chains require organizations to be responsible not only for the risks of their own activities, but also for the potential negative impacts on people and the environment.

Duarte et al. [8] emphasize that achieving sustainability in supply chains in practice requires balancing economic efficiency, environmental impacts and social justice. They also consider that in some cases prioritizing social goals can lead to compromises with economic efficiency or environmental optimization. This in turn means that sustainability in supply chains requires complex management choices between different, often competing priorities.

In this line of reasoning, digital technologies are being established as a very serious tool for overcoming some of the limitations and for improving management practices in supply chains. Qazi, Seuring and Khalid [9] emphasize the importance and role of modern technologies. According to them, the opportunities that artificial intelligence, big data and blockchain provide, give a serious opportunity to

increase transparency, traceability and efficiency in supply chains. According to scientists, there is also the opportunity to support the implementation of sustainable and socially responsible practices. In this sense, Qiao et al. [10] comment that when companies use data more actively in supply chains, they achieve more sustainable results, which is mainly due to greater transparency and better-informed decisions.

In the context of the increasing complexity of supply chains, supplier selection is becoming a critical process in which organizations must balance economic, environmental, and social criteria. According to Ziari, Soheyli, and Taleizadeh [11], the use of intelligent analytical approaches allows for a more precise assessment of suppliers, while also including additional elements such as risk of delay and sustainability of performance. Shishehgarkhaneh et al. [12] emphasize that Intelligent Recommender Systems are increasingly used in supply chains, being particularly useful for supporting complex management decisions, including supplier selection, logistics, and sustainable practices, as they provide a higher degree of transparency and adaptability. Blockchain technology is increasingly being applied in supply chains as a tool to increase transparency, efficiency, and competitiveness of companies [13]. The cited sources show that sustainability is increasingly being realized through specific analytical and technological solutions that support management decision-making.

However, with the increasing integration of artificial intelligence into supply chains, new questions arise regarding the transparency, fairness, and sustainability of decision-making. Karlsen, Mubeen, and Khan [14] draw attention to the fact that in recent years there has been an increasing use of artificial intelligence in supply chains. This in turn places additional demands on the transparency, accountability, and ethics of management decisions, especially in the absence of a unified framework for the responsible and explainable use of algorithms.

Issues of transparency and fairness of decision-making are becoming increasingly important, which is logically reflected in the increased scientific view on this topic. According to Li, Shi, Zhang and Chen [15], the application of the principles of responsible artificial intelligence can improve fairness between partners in the supply chain – both in terms of distribution and the procedures themselves, which in turn contributes to achieving competitive advantages. Park [16] also shares the opinion that the use of artificial intelligence in supply chains can contribute to achieving environmental goals, including by reducing carbon intensity and promoting circular practices. However, the scientist makes the reservation that the effects on social responsibility are not unambiguous and depend to a large extent on the presence of adequate management mechanisms and controls.

With the increasing use of AI and algorithmic management, new ethical and legal challenges related to transparency, data protection and labour rights compliance are emerging in organizations, which places additional demands on corporate responsibility in a digitalized environment [17, 18]. This broadens the understanding of

corporate responsibility to include, on the one hand, supply chain management, but also the way in which digital technologies and algorithms impact people, organizations and society.

In modern supply chains, extended corporate social responsibility is increasingly associated with issues such as supply security, process traceability, digital control and ESG compliance. Organizations are increasingly using digital technologies, data analytics, artificial intelligence and blockchain solutions to improve transparency, reduce supplier risks and ensure more sustainable and responsible supply chain management. In this sense, extended CSR is no longer seen only as an ethical or managerial approach, but also as part of the development of safer, technologically integrated and more efficient supply chain management systems.

II. MATERIALS AND METHODS

The main objective of this study is to determine how business organizations perceive the expansion of CSR in supply chains and to what extent they are inclined to integrate it or have already integrated it into supplier management processes. In addition, the impact of the new requirements of extended CSR on transparency and control of supplies is also examined. In accordance with the set objective, the study focuses on two main areas - the relationship between transparency and control in supply chains, as well as the degree of integration of extended CSR into supplier management processes. The study is based on the following two hypotheses:

H1. Higher transparency in supply chains is associated with a higher level of control over suppliers.

H2. Companies that perceive CSR as an extended responsibility integrate social and environmental criteria to a greater extent in supplier management.

For this purpose, a questionnaire was developed, through which a total of 137 people (managers at various levels, company owners, employees and supplier representatives) were surveyed between December 2025 and February 2026.

The questionnaire is divided into 5 thematic sections. The first section examines the profile of the respondent (position in the company, total years of work experience, years in the company in the last position, gender, highest level of education), and also collects information about the profile of the company for which he/she works (sector, company size, presence of international suppliers). The second section of the questionnaire is mainly related to the understanding of the extended concept of CSR, the third identifies the degree of integration of the new concept of CSR in supplier management, the fourth is dedicated to the impact on transparency and control, and the fifth identifies the challenges due to the extended CSR and new practices, as well as the opportunities it creates.

The structure of the questionnaire is presented in more depth in Table 1. As can be seen from the table, each section is aimed at measuring specific aspects of the extended CSR in supply chains.

TABLE 1. STRUCTURE OF THE QUESTIONNAIRE

THEMATIC SECTION	MAIN PURPOSE	KEY DIMENSIONS	BASIC INDICATORS	TYPE SCALE
Section 1. Profile of respondents and companies	Identifying characteristics of respondents and organizations	Demographic and organizational characteristics	Position, work experience, education, sector, company size, presence of international suppliers	Nominal/ categorical
Section 2. Understanding of extended CSR	Assessment of the perception of CSR as an extended responsibility	Perception of CSR, scope of responsibility, importance of regulations	Responsibility towards suppliers, influence of regulations, perception of CSR as a strategic factor	Likert-type scale (5-point)
Section 3. Integration in supplier management	Research on the extent of CSR implementation in supplier management	Selection, evaluation and control of suppliers	Use of social and environmental criteria, supplier monitoring, compliance requirements	Likert-type scale (5-point)
Section 4. Transparency and control	Analysis of the relationship between transparency and control	Traceability, access to information, control mechanisms	Level of transparency, controllability, use of tracking technologies	Likert-type scale (5-point)
Section 5. Challenges and opportunities	Identifying the main barriers and benefits	Constraints, Incentives, Effects	Lack of resources, coordination, regulatory pressure, competitive advantages	Likert-type scale (5-point)

Each thematic section of the survey (with the exception of Section 1, which collects information about the profile of the respondent and the organization for which he works) corresponds to specific aspects relevant to the research objective. From this perspective, the second thematic section measures the perception of CSR as an extended responsibility, the third reflects the degree of its

integration into the management processes of suppliers, and the fourth is aimed at assessing transparency and control as separate, but at the same time interrelated dimensions. The variables were measured through a set of statements, rated on a five-point Likert scale, where higher values reflect a higher degree of agreement and, accordingly, a stronger manifestation of the phenomena

under study. The main variables are defined through groups of statements, rated on a five-point Likert scale. Transparency was measured through statements related to access to information about suppliers, traceability and visibility of processes in the supply chain. Control was measured through statements related to supplier monitoring, assessment procedures and applied control mechanisms. The perception of CSR as an extended responsibility was assessed through statements exploring the understanding of corporate social responsibility as a commitment that goes beyond the organization itself. The integration of CSR into supplier management was measured through statements related to the use of social and environmental criteria in the selection, assessment and monitoring of suppliers. For each of the main dimensions studied, summary indicators were calculated as the average values of the relevant statements.

The data analysis is carried out in two main stages. In the first stage, descriptive statistics are applied in order to present a general picture of the perceptions and practices of the respondents related to extended CSR. In the second stage, the analysis is aimed at examining the relationships between the main variables in accordance with the formulated research hypotheses. Specifically, correlation analysis examines the relationship between transparency and control in supply chains (H1), as well as between the perception of CSR as an extended responsibility and the degree of its integration into supplier management processes (H2). Given the nature of the data and the Likert scales used, Spearman's correlation coefficient (Spearman's rho) was applied to test the hypotheses.

The statements used are grouped according to the main research dimensions and are developed based on the thematic areas identified in the scientific literature. Due to the limited scope of the study, no additional statistical verification of the internal consistency of the scales was conducted, which can be considered a limitation of the present study.

It should be noted that this study is limited in terms of scope and specific characteristics of the sample, therefore the results obtained should be interpreted with some caution and, respectively, cannot be fully generalized to all business organizations.

III. RESULTS AND DISCUSSION

The profile of the respondents is diverse and covers different perspectives. The data was collected through an online questionnaire, using professional contacts and business networks. The study used a non-representative targeted sampling of respondents, with the questionnaire distributed through professional contacts and business networks. Participants were selected based on their involvement in management activities, supplier relations or activities related to corporate social responsibility. Due to the specificity of the sample, the results obtained should be considered indicative of the studied group and not fully representative of all business organizations. Out of a total of 137 respondents, the majority are specialists (43%), the next largest group is formed by managers (middle and senior) – 31%, followed by representatives of suppliers –

17% and the smallest group of respondents is formed by representatives of executive level managers and owners (9%). In terms of experience, the sample largely covers more experienced representatives – the largest group according to this criterion are respondents with between 6-10 years of work experience (38%), followed by those with 11-15 years of experience (26%). Less represented are the groups of people with very long – more than 15 years of experience – 19% and those with only initial experience – 17%. – between 0-5 years. In terms of education, two almost equal groups are formed – 47% of respondents have secondary education, and another 42% have higher education. Only 11% of respondents stated that they have a lower level of education, which is easily explainable, considering the initial requirements that the respondents had to meet.

In terms of sector, the majority of the surveyed companies are in the service sector (39%), with companies related to production and industry also well represented (28%), followed by trade/retail (25%) and others (8%). In terms of company size, the largest number of representatives are large companies (46%), followed by those of medium-sized companies (31%), while small ones are represented with 23% participation in the sample. The majority of respondents stated that they use international suppliers (67%). This profile of the respondents participating in the study, as well as the enterprises they work for, allows for interesting conclusions to be drawn, related to extended corporate social responsibility.

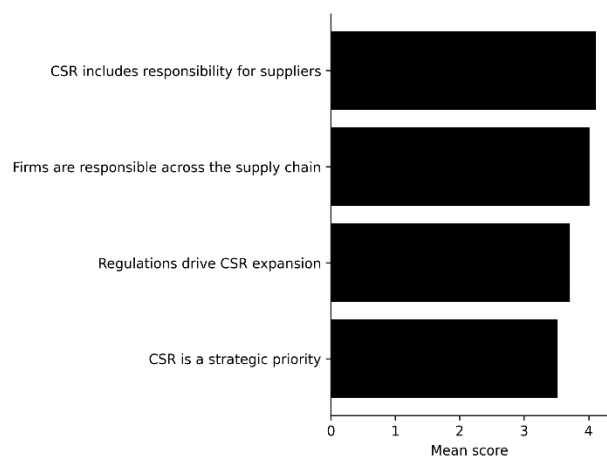


Fig. 1. Perception of Extended CSR.

The results of the second section of the survey show that respondents largely perceive corporate social responsibility as an extended requirement that goes beyond the organization itself. The average values of the main indicators range between 3.7 and 4.1, indicating a relatively high level of agreement among respondents. The high average values for the statements related to the responsibility of companies to their suppliers indicate a clear understanding that CSR should cover the entire supply chain, not just internal organizational activities.

At the same time, there is strong agreement regarding the role of regulatory requirements as a factor that further

stimulates the expansion of CSR. A significant part of the respondents share that it is the regulatory environment that contributes to the more active engagement of organizations with responsible practices towards their partners and suppliers. Therefore, among the organizations surveyed, there is a relatively high level of awareness of the extended role of CSR. This, in turn, creates prerequisites for its further implementation in management processes, including in the field of supplier management. The results related to the perception of extended CSR are presented in Figure 1.

The results of the third section of the survey provide a more in-depth understanding of the extent to which the extended concept of corporate social responsibility is applied in the practice of organizations, in particular in supplier management processes. The average value for CSR perception is 3.86, while the average value for its integration in supplier management is lower (3.41), indicating a visible gap between perception and implementation.

In general, a positive trend is observed in terms of the integration of social and environmental criteria in the selection and evaluation of suppliers. A significant part of the respondents indicated that in addition to purely economic indicators, those related to sustainability and social responsibility are considered when making decisions. This shows that the concept of extended CSR is gradually being reflected in management practices.

At the same time, however, the analysis of the data shows that the degree of actual implementation of these principles is more moderate compared to their theoretical perception. There is a certain discrepancy between the understanding of the need to integrate CSR and the specific actions related to monitoring and control of suppliers. The lower values of the indicators related to the current control and tracking of suppliers' activities suggest that this process is not yet fully developed.

This discrepancy can be explained by a number of practical constraints, such as the need for additional resources, lack of implementation due to excessive complexity of processes, as well as the lack of established control mechanisms throughout the supply chain. From this perspective, although there is a positive attitude towards extended CSR, its full integration into supplier management processes is still in the process of development. The relationship between CSR perception and its integration in supplier management is illustrated in Figure 2.

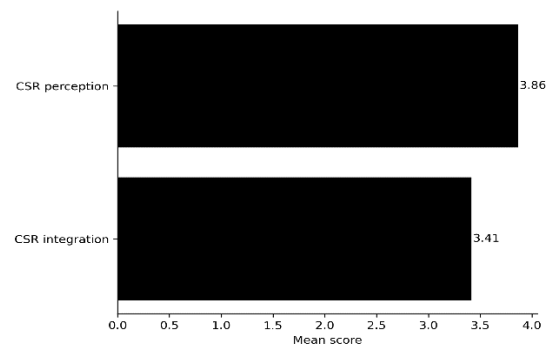


Fig. 2. Perception vs Integration in Supplier Management

The fourth thematic section is focused directly on examining the processes related to the supply chain, as well as the possibility of exercising greater control. That is, within the framework of this section, an answer is given to the question of how much the management of companies monitors what is happening in the supply chain and to what extent they can, in turn, influence and control these processes. In terms of transparency, the assessment related to access to information, traceability of supplies, as well as the level of visibility of the processes related to supplies themselves was studied. The average level of transparency is 3.72, while the level of control is lower (3.38), which confirms the presence of a gap between access to information and the ability to exercise control. After analysing the answers, the results indicate that a relatively moderate level of transparency is observed. Organizations have only basic information related to the activities of suppliers, but it does not categorically cover absolutely all elements of the supply chain. Therefore, with insufficient information, it is impossible to ensure better control in turn.

Regarding control over suppliers, the results show a rather moderate level of development of the relevant mechanisms. At present, the management of organizations has certain monitoring and evaluation tools, but what is also observed is that control is not applied to the same extent throughout the supply chain. In a number of cases, it is limited to individual stages or to key partners, which in turn does not imply the presence and application of a systematic and comprehensive approach.

On the other hand, it should also be noted that the availability of information about the activities of suppliers is not a sufficient condition for the implementation of effective control. This can be explained by the need for additional resources, clearly developed monitoring and evaluation procedures and subsequent management decision-making related to the analyses of this assessment. In this sense, it can be observed that control remains a reactive rather than a proactive management tool.

Despite the presented limitations, the data suggest the presence of a positive relationship between transparency and control, with the higher level of access to information creating prerequisites for more effective exercise of control functions. Although the relationship between transparency and control is complex, it can be concluded that transparency plays a fundamental role in improving control

in supply chains. The comparison between transparency and control is presented in Figure 3.

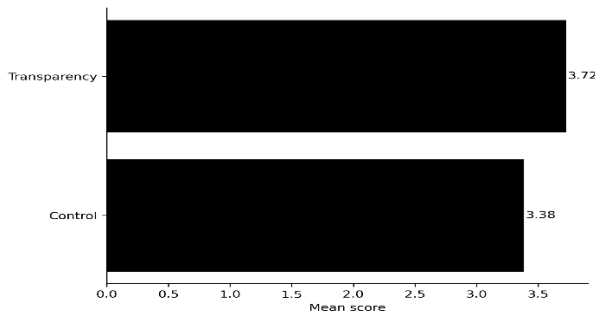


Fig. 3. Transparency and Control in Supply Chains

The fifth section is aimed at identifying the main challenges and opportunities that arise when implementing extended CSR in supply chains. The main identified barriers are related to the lack of sufficient resources; lack of effective coordination with suppliers; difficulties in controlling the entire supply chain; additional costs; additional administrative burden. The highest average values are observed for reputation benefits (3.92) and lack of resources (3.84), indicating that respondents perceive both challenges and opportunities as significant. The main challenges and opportunities identified by respondents are summarized in Figure 4.

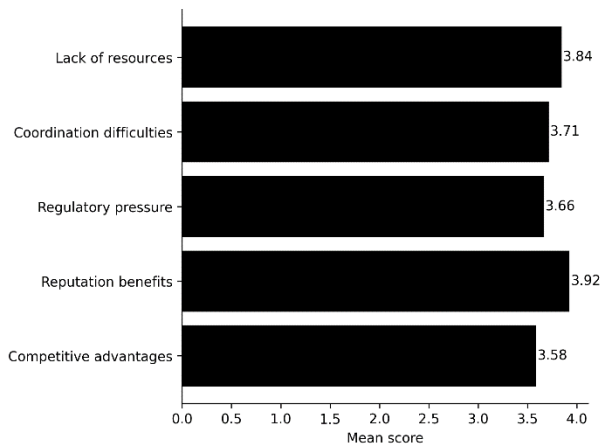


Fig. 4. Challenges and Opportunities of Extended CSR in Supply Chains

At the same time, the identified opportunities are related to better reputation; ensuring a better level of transparency; more options for choosing suppliers, creating real opportunities for achieving competitive advantage. These observations in turn lead to the conclusion that extended CSR is not perceived unilaterally only as a mandatory additional requirement or administrative burden that companies have to deal with. At the same time, extended CSR is also identified as a potential management tool for improving the sustainability and reliability of supply chains.

IV. CONCLUSIONS

The present study summarizes the main observations related to the requirements and implementation of extended CSR in the real management processes of companies.

The testing of the research hypotheses is based on correlation analysis between the main variables.

TABLE 2. CORRELATION ANALYSIS OF THE RESEARCH HYPOTHESES

Hypothesis	Variables	Correlation coefficient	Interpretation
H1	Transparency – Control	$r = 0.42$	Moderate positive relationship
H2	CSR perception – CSR integration	$r = 0.38$	Moderate positive relationship

The first hypothesis (H1), which assumes that higher transparency in supply chains is associated with a higher level of control over suppliers, finds only partial confirmation in the results of the study. The analysis shows a positive correlation between transparency and control ($r = 0.42$), indicating a moderate relationship between the two variables. This suggests that higher levels of transparency are associated with higher levels of control, although the relationship is not strong enough to indicate a strong dependency. The data show that there is a positive relationship between them, as better access to information and higher traceability create conditions for more effective control. At the same time, however, it is established that this relationship is not automatic, since the presence of transparency does not always lead to consistent and systematic application of control mechanisms.

The second hypothesis (H2), related to the statement that organizations that perceive CSR as an extended responsibility, to a greater extent integrate social and environmental criteria in supplier management, also receives partial confirmation. A positive correlation is also observed between the perception of CSR as an extended responsibility and its integration into supplier management processes ($r = 0.38$). This indicates that organizations with a stronger understanding of extended CSR tend to integrate it to a greater extent, although the relationship remains moderate. The results show a clear understanding and positive attitude towards the extended concept of CSR, which is reflected to a certain extent in management practices. However, there is a gap between the perception of CSR and its actual implementation, which indicates that the integration process is not yet fully completed.

In this line of reasoning, the extended concept of CSR has the potential to establish itself as an important management mechanism for adapting companies to the ever-growing expectations and requirements of modern society.

ACKNOWLEDGEMENTS

The publication is funded by the University of National and World Economy (Sofia, Bulgaria) under the project

NID NI-32/ 2025 on the topic: “Aspects of CSR implementation in Bulgarian conditions”.

REFERENCES

- [1] M. A. Camilleri, The rationale for responsible supply chain management and stakeholder engagement, *Journal of Global Responsibility*, Volume 8, Issue 1, 2017, Pages 111-126, ISSN 2041-2568, <https://doi.org/10.1108/JGR-02-2017-0007>.
- [2] V. Roy, B. S. Silvestre, S. Singh, Reactive and proactive pathways to sustainable apparel supply chains: Manufacturer's perspective on stakeholder salience and organizational learning toward responsible management, *International Journal of Production Economics*, Volume 227, 2020, 107672, ISSN 0925-5273, <https://doi.org/10.1016/j.ijpe.2020.107672>.
- [3] M. Damert, L. Koep, E. Guenther, J. Morris, Stakeholders and socially responsible supply chain management: the moderating role of internationalization, *Sustainability Accounting, Management and Policy Journal*, Volume 12, Issue 4, 2020, Pages 667-694, ISSN 2040-8021, <https://doi.org/10.1108/SAMPJ-03-2019-0092>.
- [4] J. Chikwana, L. Alinaghian, K. Razmdoost, Exploring sustainable purchasing and supply chain management through an institutional change lens: A systematic literature review, *Journal of Purchasing and Supply Management*, 2026, 101127, ISSN 1478-4092, <https://doi.org/10.1016/j.pursup.2026.101127>.
- [5] S. U. Hoejmoose, J. K. Roehrich, J. Grosvold, Is doing more doing better? The relationship between responsible supply chain management and corporate reputation, *Industrial Marketing Management*, Volume 43, Issue 1, 2014, Pages 77-90, ISSN 0019-8501, <https://doi.org/10.1016/j.indmarman.2013.10.002>.
- [6] B. Al-Esmael, F. Talib, M. N. Faisal, F. Jabeen, Socially responsible supply chain management in small and medium enterprises in the GCC, *Social Responsibility Journal*, Volume 16, Issue 3, 2019, Pages 369-386, ISSN 1747-1117, <https://doi.org/10.1108/SRJ-09-2017-0174>.
- [7] C. M. Both, M. Wilhelm, Supply chain sustainability risk management in the era of mandatory due diligence: A literature review, *Journal of Purchasing and Supply Management*, Volume 32, Issue 2, 2026, 101083, ISSN 1478-4092, <https://doi.org/10.1016/j.pursup.2025.101083>.
- [8] I. Duarte, B. Mota, T. Pinto-Varela, A. Amaro, S. Moniz, A. P. Barbosa-Povoa, Socially responsible pharmaceutical supply chains for equitable access, *Socio-Economic Planning Sciences*, Volume 105, 2026, 102493, ISSN 0038-0121, <https://doi.org/10.1016/j.seps.2026.102493>.
- [9] S. A. Qazi, S. Seuring, R. U. Khalid, Bridging digital features and sustainability, through social capital in supply chain management: insights from X analytics, *The International Journal of Logistics Management*, Volume 37, Issue 2, 2025, Pages 500-519, ISSN 0957-4093, <https://doi.org/10.1108/IJLM-03-2025-0172>.
- [10] J. Qiao, A. Appolloni, M. Wu, Y. Cai, Z. Cui, Integrating transparency and circular economy principles into data-driven agrifood supply chains for environmental management, *Journal of Environmental Management*, Volume 404, 2026, 129230, ISSN 0301-4797, <https://doi.org/10.1016/j.jenvman.2026.129230>.
- [11] M. Ziari, A. Soheyli, A. A. Taleizadeh, An intelligent analytics framework for supplier selection and delay risk management in sustainable supply chains, *Supply Chain Analytics*, Volume 14, 2026, 100208, ISSN 2949-8635, <https://doi.org/10.1016/j.sca.2026.100208>.
- [12] M. B. Shishehgharkhaneh, R. Moehler, Y. Fang, A. A. Hijazi, H. Aboutorab, A. J. Dhamankar, Application of recommender systems in supply chain management: A state-of-the-art review, *Intelligent Systems with Applications*, Volume 30, 2026, 200661, ISSN 2667-3053, <https://doi.org/10.1016/j.iswa.2026.200661>.
- [13] I. Dimitrov and R. Gigov, Increasing the Supply Chain Competitiveness of Bulgarian Companies by Applying Blockchain Technology, 2022 V International Conference on High Technology for Sustainable Development (HiTech), Sofia, Bulgaria, 2022, pp. 1-4, doi: 10.1109/HiTech56937.2022.10145534.
- [14] E. H. Karlsen, R. Mubeen, M. Khan, Responsible AI in Project and Supply Chain Management: A Scoping Review of Governance Mechanisms and Ethical Guidelines (2010–2025), *Procedia Computer Science*, Volume 278, 2026, Pages 1760-1767, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2026.03.167>.
- [15] L. Li, R. Shi, R. Zhang, L. Chen, How can firms leverage responsible artificial intelligence to build competitive advantages? The role of supply chain justice and complexity, *International Journal of Production Economics*, Volume 297, 2026, 110010, ISSN 0925-5273, <https://doi.org/10.1016/j.ijpe.2026.110010>.
- [16] M. J. Park, Generative AI and responsible supply chains: When sustainability gains undermine social legitimacy, *Technology in Society*, Volume 85, 2026, 103240, ISSN 0160-791X, <https://doi.org/10.1016/j.techsoc.2026.103240>.
- [17] M. Angelova, Ethical and Legal Implications of Algorithmic Management, 2025 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5, doi: 10.1109/COMSCI67172.2025.11225221.
- [18] M. Angelova, Algorithmic Management in the Gig Economy: ICT Infrastructures and Ethics, 2025 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-6, doi: 10.1109/COMSCI67172.2025.11225162.

CSR and Employee Well-Being in Sustainable Human Resource Management

Kiril Anguelov
Management and Business
Information Systems
Technical University of Sofia
Sofia, Bulgaria
ang@tu-sofia.bg

Philip Stoyanov
Management Department
University of National and World
Economy
Sofia, Bulgaria
ph.stoyanov@unwe.bg

Rima Tamošiūnienė
Financial Engineering Department
Vilnius Gediminas Technical
University
Vilnius, Lithuania
rima.tamosiuniene@vgtu.lt

Abstract— This report analyses the role of corporate social responsibility in the formation and development of human capital in organizations, emphasizing employee well-being as a fundamental and mandatory stage in achieving sustainable organizational development. The analysis examines contemporary approaches through which companies integrate mental health policies, work-life balance and employee engagement within their CSR strategies. On this basis, it is argued that employee well-being, in addition to being part of corporate social responsibility, is also becoming an indispensable part of the strategic resource of the business organization for increasing productivity, innovation potential and long-term competitiveness of organizations.

Keywords— Corporate social responsibility; well-being, sustainable HRM.

I. INTRODUCTION

In the extremely complex business environment in which business companies operate, with the complicated geopolitical situation and its economic consequences, the ability to form and retain a quality team is becoming increasingly important as one of the main prerequisites for the competitiveness of companies. In recent years, companies have been paying special attention and developing comprehensive strategic policies related to the management of intangible assets and, in particular, human capital. At the same time, CSR is also undergoing evolutionary development - from a concept focused mainly on external responsibility and society as a whole, the scope is expanding and now largely covers internal stakeholders. In this sense, it can be said that a transformation is being observed from social responsibility to sustainable human resources management. Despite the undeniable imposition of the concept of CSR, employee well-being, in turn, often remains only at the level of good-sounding formulations in CSR strategies, without, however, finding practical

application and being truly integrated into HRM. In many organizations, employee well-being policies are linked to the broader concept of CSR, but many of them are not reflected in the daily activities of HR. This leads to a discrepancy between stated organizational priorities and actual practices. In most cases, if there is one at all, well-being is perceived as a form of complementary initiative with a non-binding nature, and it is not seen as a real mechanism for human resources management at all. As a result, there is very little interaction and integration between CSR and HRM, which weakens the ability of organizations to develop employee well-being as one of the important factors for achieving sustainable development and long-term competitiveness. In this sense, this report explores and analyses the way in which CSR integrates the concept of well-being, including the links between implemented policies and their real results. On this basis, working mechanisms for impact and a stronger connection between CSR and well-being have been identified.

II. LITERATURE REVIEW

In the contemporary scientific literature, employee well-being is considered as one of the main elements in human resource management and at the same time as an essential component of the overall concept of corporate social responsibility. There is an increasingly clear understanding that organizations cannot achieve sustainable development without targeted policies and practices aimed at internal stakeholders, on whom they mainly rely to achieve competitiveness and sustainability. However, a number of studies question the effectiveness of existing approaches, emphasizing the discrepancy between formulated strategies and their actual implementation, as well as the need for a more in-depth study of the interrelationships through which organizational practices affect employee well-being.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.183>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

Saleh, Koburtay and Staniszewska [1] reveal that the effectiveness of work-life balance practices depends to a large extent on the coherence between formulated policies and the actual behavior of managers. When there is a discrepancy, these practices may be perceived not as a resource but as an additional requirement, which directly limits their impact on employee well-being. At this point Odame et al. [2] comment that employee well-being initiatives are often perceived as superficial when they do not reflect their real needs. In these cases, employees believe that they are used as a tool for organizational image rather than for their own benefit. This observation actually highlights the importance of trust, authenticity and active employee involvement to achieve real impact.

These observations raise the question of why such a discrepancy exists between formulated policies and actual results. According to Messersmith [3], most of the links between HR practices and employee well-being are built on limited models that focus mainly on social exchange and organizational effectiveness. In reality, such an approach significantly limits the concept of well-being to indicators such as satisfaction and engagement and does not take into account its deeper dimensions. In this sense, the author argues for the need for a reorientation towards approaches that consider well-being through the logic of autonomy, competence and social connectedness.

From this perspective, the need to analyse the mechanisms through which management practices affect employee well-being is increasingly emerging. Mou, Rasoolimanesh, and Chuah [4] believe that the relationship between corporate social responsibility and employee well-being is not direct, but is realized through intermediate mechanisms, such as the perception of organizational justice. According to scientists, this means that the effects of CSR on employees depend to a significant extent on the way in which organizational policies are transformed from strategic documents into actual management practices.

In addition to the perception of justice, a number of studies identify other organizational factors that mediate this relationship. Dutta, Poyil, and Vedak [5] prove that organizational support is a significant link between management practices and employee well-being, enhancing the effect of commitment and flexible working arrangements on their results.

Giovanis, Özdamar and Ozdamar [6] comment that the effects on employee well-being depend heavily on the availability of organizational resources such as managerial support, autonomy and work-life balance. This observation also highlights the role and importance of the actual implementation of management practices.

Along with the favourable opportunities, the scientific literature also outlines a number of negative processes that can undermine employee well-being. Kanwal et al. [7] draw attention to the fact that unfavourable organizational conditions can form a perception of injustice, which in turn leads to behavioural reactions such as silence and ultimately has a negative impact on employee well-being.

In addition to organizational factors, individual psychological perceptions also play a significant role. Diao

et al. [8] emphasize that the impact of management practices on employee well-being is realized through various mechanisms, such as a sense of meaning in work, which emphasizes the role of subjective perception in the formation of well-being.

Xerri and Rafferty [9] conclude that employee well-being is influenced not only by formal management practices, but also by the accumulation of internal psychological resources, such as psychological capital. According to scientists, it is this capital that plays a key role in dealing with uncertainty and changes in the organizational environment.

At the same time, well-being is not formed solely through formal policies and structures. Charki et al. [10] state that employee well-being is formed initially through formal organizational practices, but subsequently - also through informal interactions, such as knowledge sharing and social support within the organizational environment.

The modern organizational environment further complicates these processes, especially in the context of increased digitalization. Recent discourse also confirms that artificial intelligence is rapidly transforming complex operational systems, suggesting that similar changes in work organization increasingly affect employee well-being and managerial practices [21]. Pham and Pham [11] comment that employee well-being is extremely influenced by emerging factors related to technological changes. They believe that organizational support should be considered as a tool for mitigating the negative effects on employees. In this sense, well-being can be commented on as a strategic opportunity for organizations in conditions of dynamic digital transformation [20]. A similar conclusion is reached by Nguyen et al. [12], who also believe that employee well-being is also formed in the context of interaction with new technological solutions. According to them, the organizational environment and employee perceptions are extremely important for achieving positive psychological outcomes. In turn, Mansuroğlu and Smith [13] state that the digitalization of the work environment is associated with new sources of stress, such as overload and blurring of the boundaries between work and personal life. This in turn has a very negative impact on employee well-being and places additional demands on organizational practices. According to Angelova [14,15], the use of artificial intelligence in Human Resource Management creates both opportunities for increasing objectivity, but also risks related to perceptions of fairness and protection of employee rights, which requires a balanced approach between technological solutions and human judgment.

A study by Sedaghati et al. [16] proves that digital forms of support can contribute to improving the emotional well-being of employees by reducing barriers to access to help and complementing traditional organizational mechanisms. Ultimately, the accumulated empirical evidence allows employee well-being to be considered on the one hand as an outcome, but on the other hand – as a factor with direct significance for organizational results.

The idea that well-being has the potential to become a strategic value for the organization is also shared by Gao

and Gu [17], who studied the relationship between leadership behaviour and employee creativity. They concluded that leadership behaviour oriented towards others (stewardship) has a positive effect on employee well-being, which in turn leads to higher creativity. Therefore, well-being has a direct role in organizational results and from this point of view can be commented on as a strategic element [19]. Poonam and Sengupta [18] believe that employee well-being has a direct positive relationship with their performance, which confirms its role as a factor of real importance for organizational effectiveness.

As a result of the analysis of the scientific literature, we can conclude that employee well-being is not an automatic result of the implementation of corporate policies. Rather, it is perceived as a complex process due to the interaction between organizational practices, individual perceptions and the specific characteristics of the internal and external environment. The presence of intermediate mechanisms, such as perception of justice, organizational support and meaning in work, emphasizes the need for deeper integration between CSR and human resource management. From this perspective, employee well-being is established as part of the strategic development of HRM, which has a direct impact on organizational efficiency and competitiveness.

III. METHODOLOGY

The main objective of this report is to examine the extent to which organizations integrate employee well-being practices within the broader concept of CSR, and how this impacts organizational performance.

To achieve this objective, the following two hypotheses were formulated:

H1: Organizations that have formal CSR policies are more likely to implement employee well-being practices.

H2: Higher levels of actual implementation of employee well-being practices are positively related to perceived organizational performance.

To test the hypotheses defined above, we conducted a survey using purposive sampling. The survey was distributed online and sent to 95 pre-selected business organizations. The purpose of this pre-selection was to ensure that at least from public information, these organizations had some policies and/ or initiatives related to CSR and ESG, and to ensure the inclusion of organizations from different economic sectors. At the same time, additional requirements for business companies were to develop part of their activities in Bulgaria, to have no less than 10 employees. It is important to emphasize that the questionnaire was not anonymous, but we required a clear indication of the name of the business organization itself and the position of the respondent, and for this goal the potential respondents were duly informed, including for what purpose this data was collected. The logical framework of the preliminary selection was to achieve expertise, as well as to comply with our preliminary

requirements, which were that one organization should be represented by only one questionnaire.

The survey was conducted during the period February - March 2026, with the longer period for online questionnaire of information gathering being associated with more efforts by the team to reach representatives of companies from the target sample. 53 organizations participated in the final sample of the survey - i.e. we received this number completed questionnaires.

The questionnaire included 5 main blocks of questions, grouped as follows: Block 1: Organization profile and respondent profile; Block 2: CSR internal orientation; Block 3: Employee well-being practices; Block 4 - Actual implementation of CSR and well-being practices; Block 5 - Perceived effects of the implementation of CSR and well-being practices.

The collected data were processed through descriptive statistics and comparative analysis, allowing for a summary of the characteristics of the sample and the degree of implementation of the practices under consideration. To test the formulated hypotheses, a correlation analysis was applied, aimed at establishing the relationships between the level of integration of employee well-being practices and perceived organizational outcomes.

IV. RESULTS

As can be seen from Table 1, the structure of the organizations participating in the study is relatively balanced, especially in terms of size. Medium-sized organizations have the largest representation (nearly 40%), followed by small ones, with a share of 34%, and large ones are the least represented – with a share of about 26%. In terms of the economic sector in which they operate, the largest share is held by companies from the service sector (32.1%), followed by ICT (20.8%), Manufacturing (18.9%), Trade (17.0%). In terms of whether there is an HRM unit or department within the business organization, 73.6% state that their organization has a separate such internal structure and only 26.4% answer negatively. This result is actually logical, considering the size of the surveyed organizations and the purposeful lack of micro-firms in this sample. The focus of the present study, related to the presence of a CSR policy, is interesting – about half (45.3%) state that the organization they represent has a developed formal CSR policy. On the other hand, a relatively high percentage – 32.1% state that they have only partially formalized such a policy, and the rest (22.6%) comment that such a policy is informal or they are not aware of its existence at all. When analyzing the answers, the profile of the respondents themselves must also be considered: nearly 40% of them are representatives of the middle management level, followed by HR experts or HR managers (nearly 36%), with the smallest share being representatives of the top management or direct owners of the surveyed companies. The resulting profile, both at the organizational level and at the personal level, will allow the collected information to be reliable and valid.

Table 1. Profile of participating organisations

Characteristic	Category	Number of organizations	Share (%)
Company size	Small (10 – 49 employees)	18	34.0
	Medium (50 – 249 employees)	21	39.6
	Large (250 + employees)	14	26.4
Sector	Services	17	32.1
	ICT	11	20.8
	Manufacturing	10	18.9
	Trade	9	17.0
	Other	6	11.3
HR function	Yes	39	73.6
	No	14	26.4
CSR policies	Formalized	24	45.3
	Partially formalized	17	32.1
	Informal / none	12	22.6
Respondent position	HR specialists/ HR managers	19	35.8
	Middle management	21	39.6
	Senior management / owners	13	24.5

Further analysis of the results shows some differences between organizations according to the sector in which they operate. There is a tendency for companies in the service and information technology sectors to report a higher level of implementation of practices related to employee well-being. To explore potential sector differences, average implementation scores for employee well-being practices were calculated for each sector (Table 2).

Table 2. Sector differences in employee well-being implementation

Sector	Main implementation score
Services	4.1
ICT	4.3
Manufacturing	3.8
Trade	3.5
Other	3.7

A possible explanation for this is the higher dependence of these organizations on human capital, as well as the increased competition for attracting and retaining qualified personnel. On the other hand, in manufacturing enterprises and organizations in the field of trade, such practices appear to be less developed or more limitedly integrated. Although the current analysis does not aim to conduct a detailed

sectoral comparison, the observed differences outline an interesting direction for future research.

The next step in the analysis is to test the first hypothesis, examining the relationship between the presence of formalized CSR policies and the implementation of employee well-being practices.

In order to reach a reasoned conclusion regarding the first hypothesis, the respondents were asked the following several questions, which are now considered in the analysis. First, there is the closed question “Does your organization have formalized CSR policies?”, with the possible answers to this question being “Yes – formalized”; “Partially formalized” and “Informal / none”. Subsequently, the respondents were asked to respond on a 5-point Likert scale to the following statements:

- Our organization actively supports employees’ mental well-being
- Work-life balance is encouraged and supported
- Flexible work arrangements are implemented in practice
- Employee engagement initiatives are regularly applied
- Managers actively support employee well-being
- There are effective channels for employee feedback

Based on the statements, we calculated the average value, with the range between 1.0 – 2.5 – being low; 2.6 – 3.7 is average, and between 3.8 and 5.0 is high. That is, the degree of implementation of practices related to employee well-being was measured by an aggregate indicator formed on the basis of the respondents’ answers to several statements, rated on a five-point Likert scale. On this basis, the organizations were classified into three groups – with a low, medium and high level of implementation of the considered practices. As a result, the data are presented in Table 3.

Table 3. CSR policies and implementation of employee well-being practices

CSR policies	Low implementation	Medium Implementation	High implementation
Formalized (24)	3	8	13
Partially formalized (17)	5	9	3
Informal / none (12)	7	4	1

The data presented in Table 3 show a clear difference between business organizations, depending on the degree of formalization of CSR policies. Organizations with formalized CSR policies have the highest share of actual implementation of employee well-being practices, with more than half of them falling into the group with a high level of implementation. This can be interpreted as an indication that the formalization of policies creates clearer conditions and leads in practice to a commitment on the part of management for their subsequent practical implementation. That is, once they are written, adopted and

announced, management, in turn, has a much greater commitment to implement them in practice.

In contrast, organizations without formalized or informal CSR policies have low levels of implementation of such practices, which suggests that in the absence of a structured policy, initiatives related to employee well-being remain rather episodic and without systematicity. In the group with partially formalized policies, an intermediate position is observed, with medium levels of implementation dominating. This fact can be explained by the incomplete integration of these policies into management practices.

The observed trend confirms that the degree of formalization of CSR policies is related first of all to their presence, and subsequently - to the commitment and depth of their actual implementation. In this sense, it can be assumed that formalized CSR policies function more as a mechanism for transforming strategic intentions into specific management actions aimed at employee well-being. On this basis, hypothesis H1 can be confirmed.

Based on the results obtained, it can be concluded that the presence of formalized CSR policies is a significantly important factor for the actual implementation of practices aimed at employee well-being. Organizations with a higher degree of formalization demonstrate significantly more active and systematic implementation of such practices, which allows hypothesis H1 to be confirmed.

To explore Hypothesis 2, which focuses on the relationship between the extent of implementation of well-being practices and perceived organizational outcomes. The extent of perceived organizational outcomes was measured by aggregating respondents' responses to several statements related to engagement, employee retention, productivity, and organizational environment (Table 4). The statements were rated on a 5-point Likert scale (1 – strongly disagree, 5 – strongly agree).

Table 4. Indicators for perceived organizational performance

Element	Statements
Employee engagement	Employees in our organization demonstrate a high level of engagement in their work. Employees are willing to go beyond their formal job responsibilities.
Employee retention	Employee turnover in our organization is relatively low. The organization is successful in retaining key talent.
Productivity and efficiency	Employees demonstrate high levels of productivity in their daily work. Work processes are carried out efficiently and with minimal disruptions.
Organizational climate	The working environment in the organization is positive and supportive. There is a high level of trust between employees and management.
Innovation and development	Employees actively contribute ideas for improvement and innovation.

	The organization encourages creativity and experimentation.
Overall performance	Overall, our organization performs effectively in achieving its objectives.

To test the relationship between the implementation of employee well-being practices and organizational performance, a correlation analysis was conducted. The results obtained show a moderately strong positive relationship between the two variables ($r = 0.62$).

This means that organizations that implement practices aimed at employee well-being to a higher extent also report better organizational performance. The relationship is strong enough to assume that such practices are not only social in nature, but also create real added value for organizations.

Based on the results obtained, a positive relationship can be established between the level of implementation of practices related to employee well-being and perceived organizational performance. The observed relationship shows that organizations with a higher level of implementation of such practices report better results. This allows us to assume that hypothesis H2 is confirmed.

The results of the study show that employee well-being practices can hardly be considered as complementary or peripheral initiatives. On the contrary, they are gradually becoming part of the toolkit of modern human resource management. In practical terms, organizations should focus their efforts on measures that have a direct impact on the daily experience of employees – maintaining a balance between work and personal life, active feedback mechanisms, flexible forms of work organization and support for mental well-being. The findings indicate that some practices may play a more noticeable role than others. Support for mental well-being, flexibility in work arrangements and opportunities for regular feedback seem particularly relevant, as they shape employees' perceptions of support and contribute to stronger engagement. The real effect of such policies depends not so much on their formal presence, but on the degree to which they become part of organizational practice.

Along with the results obtained, it is necessary to consider some limitations of the present study. First of all, the sample used is relatively limited in size and was formed through purposeful selection, which places certain limitations on the possibility of a broader generalization of the results. In addition, the study is mainly aimed at organizations where there are at least indications of the presence of initiatives or policies related to corporate social responsibility. This does not allow for a clearer comparison with organizations where such practices are absent. Additionally, some of the analyzed indicators are based on subjective assessments of the respondents, and not on objective organizational indicators such as turnover, absences, financial results or other measurable indicators. Future studies could expand the scope of the analysis through larger samples, inclusion of control groups and use of additional objective indicators.

V. CONCLUSION

This report aimed to examine the extent to which organizations integrate employee well-being practices within a more general and targeted policy related to corporate social responsibility, as well as to assess their impact on organizational performance. In the context of the ever-increasing role and importance of intangible resources in achieving sustainable development, this issue is becoming increasingly relevant and the management of modern business organizations is “forced” to pay more and more attention.

The results of the study allow us to draw several main conclusions. First of all, we can comment that there is a clear relationship between the presence of formalized CSR policies and the degree of implementation of employee well-being practices. Organizations that have clearly defined policies demonstrate a significantly higher level of commitment to their implementation and, therefore, the actual implementation of such practices.

Secondly, the results show a positive relationship between the degree of implementation of employee well-being practices and perceived organizational performance. This leads to the conclusion that organizations that invest purposefully in the well-being of their employees report better results in terms of engagement, productivity and overall effectiveness.

The results obtained allow for a slightly broader interpretation of the role of employee well-being in the overall policy of modern organizations. The data show that employee well-being has the potential to become a real management tool through which organizations can influence their results.

At the same time, it should be noted that the opportunities for implementing such practices are not the same in different organizations. Small enterprises often have limited resources and can therefore rely on more flexible and low-budget solutions, such as feedback, working time organization or informal support mechanisms. Medium-sized enterprises have the opportunity to gradually integrate such initiatives into more structured human resource management policies. In large organizations, there are already prerequisites for building more comprehensive systems, including specialized employee support programs and integrating well-being indicators into the broader organizational strategy.

In recent years, a clear transformation has been observed - from the perception of CSR as an externally oriented activity to something much more complex and equally focused on internal stakeholders - in particular human resource management. This places employee well-being in the position of a strategic tool that is able to support the sustainable development of the company and contribute to increasing its competitiveness and long-term effectiveness.

ACKNOWLEDGEMENTS

The publication is funded by the University of National and World Economy (Sofia, Bulgaria) under the project

NID NI-32/ 2025 on the topic: “Aspects of CSR implementation in Bulgarian conditions”.

REFERENCES

- [1] R. M. Saleh, T. Koburtay, Z. Staniszewska, Leadership, work-life balance and employee well-being in Dubai's service industries: implications for HRM, *Personnel Review*, Volume 55, Issue 1, 2026, Pages 107-133, ISSN 0048-3486, <https://doi.org/10.1108/PR-06-2025-0663>.
- [2] D. A. Odame, W. Laube, R. E. Hinson, E. Dzandu, Exploring employee perspectives about well-being initiatives by formal sector organisations in Ghana during the COVID-19 pandemic, *Employee Relations: The International Journal*, Volume 47, Issue 8, 2025, Pages 1311-1329, ISSN 0142-5455, <https://doi.org/10.1108/ER-08-2024-0446>.
- [3] J. G. Messersmith, HRM systems & employee well-being: Toward a eudaimonic perspective, *Human Resource Management Review*, Volume 36, Issue 3, 2026, 101149, ISSN 1053-4822, <https://doi.org/10.1016/j.hrmr.2026.101149>.
- [4] W. Mou, S. M. Rasoolimanesh, S. H.-W. Chuah, When fairness prevails: unpacking the mediating mechanism linking corporate social responsibility, hotel employees' quality of work life and well-being, *Social Responsibility Journal*, Volume 22, Issue 3, 2026, Pages 551-572, ISSN 1747-1117, <https://doi.org/10.1108/SRJ-04-2025-0336>.
- [5] D. Dutta, A. K. Poyil, C. Vedak, Examining HRM practices emerging out of COVID-19 in the MSME sector: impact of employee engagement, perceived organizational support and well-being, *Employee Relations: The International Journal*, Volume 47, Issue 7, 2025, Pages 1088-1105, ISSN 0142-5455, <https://doi.org/10.1108/ER-07-2024-0383>.
- [6] E. Giovanis, B. Özdamar, O. Ozdamar, Managing digital work in the post-pandemic era: telework intensity, organisational support, and employee well-being, *International Journal of Workplace Health Management*, Volume 19, Issue 2, 2025, Pages 150-171, ISSN 1753-8351, <https://doi.org/10.1108/IJWHM-09-2025-0245>.
- [7] N. Kanwal, G. Hussain, A. S. N. Isha, Al-B. A. Al-Mekhlafi, The sequential association of perceived organizational injustice and employee silence between psychosocial issues and health and well-being, *International Journal of Workplace Health Management*, Volume 18, Issue 6, 2025, Pages 558-577, ISSN 1753-8351, <https://doi.org/10.1108/IJWHM-03-2025-0056>.
- [8] R. Diao, W. Chang, A. Liu, M. Wang, Q. (C.) Yang, Sensemaking as a bridge between authentic leadership and employee well-being: a multilevel model of work meaningfulness and group empathy, *International Journal of Contemporary Hospitality Management*, Volume 38, Issue 1, 2025, Pages 366-385, ISSN 0959-6119, <https://doi.org/10.1108/IJCHM-03-2025-0410>.
- [9] M.J. Xerri, A. Rafferty, Psychological capital accumulation and depletion during organisational change: consequences for employee well-being, *Personnel Review*, Volume 55, Issue 1, 2026, Pages 175-192, ISSN 0048-3486, <https://doi.org/10.1108/PR-11-2024-1035>.
- [10] M. H. Charki, N. Boukef, J. Benítez, S. You, A. Mehra, L. P. Robert, Knowledge contribution on enterprise social media and employee well-being, *Information & Management*, Volume 63, Issue 3, 2026, 104302, ISSN 0378-7206, <https://doi.org/10.1016/j.im.2026.104302>.
- [11] T. N. N. Pham, H. H. Pham, Protecting employee well-being in the age of AI: Empirical evidence from vietnam's hospitality sector, *Strategic Business Research*, Volume 2, Issue 1, 2026, 100052, ISSN 3051-0643, <https://doi.org/10.1016/j.sbr.2026.100052>.
- [12] M. Nguyen, T. P. Nham, R. Alghafes, O. Rahman, G. Imre, Human-GenAI-based agent collaboration: How employee perceptions shape knowledge sharing, thriving, and well-being, *Acta Psychologica*, Volume 263, 2026, 106271, ISSN 0001-6918, <https://doi.org/10.1016/j.actpsy.2026.106271>.
- [13] E. Mansuroğlu, A. P. Smith, Technostress and employee well-being: A systematic review of empirical evidence, *Computers in*

Human Behavior Reports, Volume 21, 2026, 100941, ISSN 2451-9588, <https://doi.org/10.1016/j.chbr.2026.100941>.

- [14] M. Angelova, Pros And Cons of Using Algorithmic Management In Human Resource. (2024). ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the International Scientific and Practical Conference, 2, 22-28.
<https://doi.org/10.17770/etr2024vol2.8031>
- [15] M. Angelova, "Ethical and Legal Implications of Algorithmic Management," 2025 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5, <https://doi.org/10.1109/COMSCI67172.2025.11225221>.
- [16] F. Sedaghati, A. Stetsenko, I. O. McMillan, H. Nagra, Z. Dana, Use of Digital Peer Support for Employee Well-Being: Retrospective Analysis Across Five Large Employers, JMIR Human Factors, Volume 13, 2026, ISSN 2292-9495, <https://doi.org/10.2196/90431>.
- [17] H. Gao, Q. Gu, Does leader stewardship behavior affect employee creativity? Roles of other orientation and employee well-being, Personnel Review, Volume 55, Issue 1, 2026, Pages 310-329, ISSN 0048-3486, <https://doi.org/10.1108/PR-07-2024-0652>.
- [18] S. Poonam, S. Sengupta, The moderating role of workplace spirituality in the relationship between employees' psychological well-being and job performance, Journal of Management Development, Volume 44, Issue 5, 2025, Pages 664-675, ISSN 0262-1711, <https://doi.org/10.1108/JMD-01-2025-0005>.
- [19] M. Chipriyanov, G. Chipriyanova, R. Krasteva-Hristova, A. Atanasov, K. Luchkov, Researching the Impact of Corporate Social Responsibility on Economic Growth and Inequality: Methodological Aspects. Journal of Risk and Financial Management, 17(12), 546, 2024.
<https://doi.org/10.3390/jrfm17120546>
- [20] K. Luchkov, G. Chipriyanova, M. Chipriyanov, (2025). Industry 5.0 and Green Transition - Challenges and Opportunities for Business and Society. In: El Khatib, M., Alzoubi, H.M., Angelova, Y. (eds) Sustainable Innovation for Engineering Management (SIEM). ISCME 2024. Advances in Science, Technology & Innovation. Springer, Cham.
https://doi.org/10.1007/978-3-031-89889-1_1
- [21] V. Zinoviev, D. Koeva, P. Tsankov, R. Kutkarska, Review of Artificial Intelligence Applications in the Digital Energy and Renewable Energy Infrastructures. Energies 2026, 19, 1250.
<https://doi.org/10.3390/en19051250>

Algorithmic Management as a Driver of Accelerated Growth in High-Growth Firms

Kiril Anguelov

Management and Business Information Systems
Technical University - Sofia
Sofia, Bulgaria
ang@tu-sofia.bg

Miglena Angelova

Management Department
University of National and World Economy
Sofia, Bulgaria
m.angelova@unwe.bg

Abstract— The focus of this report is on exploring the relationship between algorithmic management and the specifics of high-growth firms, emphasizing the mechanisms through which data and algorithms support the achievement of accelerated organizational development. The analysis examines the role of artificial intelligence in decision-making processes, resource optimization, and adaptation to a dynamic business environment. On this basis, the main management mechanisms through which algorithmic management can function as a growth factor are identified, as well as limitations related to data dependence, transparency, and ethical aspects of algorithmic management.

Keywords— *Algorithmic Management, Fast Growing Company, Artificial Intelligence, Accelerated Growth.*

I. INTRODUCTION

With the development of ICT and the ever-deepening digital transformation, business organizations are faced with increasingly new opportunities to achieve competitive advantage and generate added value from their activities. One of the most relevant aspects of the extremely rapidly developing digitalization and ICT is the rapid penetration of AI into various business processes, including those related to management. From this perspective, algorithmic management has increasingly begun to gain popularity as a new management model that is capable of rethinking and rearranging the entire traditional management logic. Expanding application of artificial intelligence across complex infrastructures and managerial systems, highlight its growing strategic role in organizational performance improvement [21].

Algorithmic management is able to provide rapid management solutions, which is especially important for fast-growing companies in order to maintain the pace and speed of their development. These solutions can lead to scalability and efficiency in the conditions of a rapidly changing business environment and high intensity of the sector.

This report is aimed at examining the relationship between algorithmic management and obtaining and maintaining accelerated company growth. From this perspective, algorithmic management should be viewed not only from its technological side, but also as a method for transforming management processes and accelerating the growth of companies [18]. At the same time, accelerated growth increasingly depends on strategic personnel development capable of adapting to data-driven and algorithmically coordinated work environments [20].

II. LITERATURE REVIEW

Nhan and Thu [1] conducted a bibliometric analysis of the scientific literature related to algorithmic management. They commented that research on this topic has increased significantly in recent years. At first, researchers paid more attention to the technical aspects of algorithmic management, while now the discourse is focused on how algorithmic management affects people, organizations in general, and their management.

This logically leads attention to research examining the impact of algorithmic management on people and teams. According to Liu and Yuan [2], the introduction of algorithmic management creates prerequisites for strengthening the resilience of teams by stimulating informal leadership and increasing employee confidence. Scientists pay special attention to the fact that the transparency of algorithms is of particular importance for the manifestation of this prerequisite, which enhances the positive effect on team dynamics.

At the same time, however, other studies report opposite results. Moritz et al. [3] conducted a meta-analysis related to determining people's reactions to algorithmic decision-making in human resource management. They came to the idea that employees are generally skeptical of decisions made by algorithms - they have less trust and consider them more unfair. According to scientists, this directly reflects on the overall attitude of employees towards the organization and a direct decrease in their

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.178>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

motivation and desire to work in the given company in general.

These contradictory effects suggest the need for a more in-depth analysis of the conditions under which algorithmic management is implemented and operates. According to Hajiheydari and Delgosha [4], the effects that algorithmic management achieves are not uniform. Its specific manifestations depend on the combination of the characteristics of the work environment and the individual characteristics of employees. In this sense, the impact of algorithms on organizational results should not be considered a universal good, since it depends extremely much on the specific conditions in the organization itself.

In these conditions, the interactions between algorithms and human behavior acquire great importance for the actual manifestation of algorithmic management. From the point of view of the interaction between algorithms and people, Zhao and Syed [5] comment that people do not simply obey algorithms, but actually develop and implement active adaptation strategies through which they try to adjust to the way algorithms work. Which logically leads to the conclusion that the impact of algorithms on the results achieved by the organization is actually based on the interaction between technologies and human behavior.

This interaction also explains the emergence of nonlinear effects in the organizational environment. Jianu, Tussyadiah and Miller [6] recognize that algorithmic management can improve certain aspects of the work environment. At the same time, however, its implementation can lead to resistance among employees, which has a negative impact on their well-being and increases the likelihood of leaving. Scientists comment that the effects of algorithms are nonlinear and depend on the balance between the constraints and benefits they create.

A similar logic is also observed in the conditions of a specific organizational environment. Liu, Yang and Liu [7], after a thorough analysis of the behavior of people employed in the gig economy, come to the conclusion that algorithmic management is able to make employees take more risks, related to the way in which the algorithm exercises control. At the same time, however, the scientists emphasize that certain personal characteristics and under certain conditions these negative effects can be limited.

Additionally, the way algorithms are implemented in organizational management and organizational processes also has a very strong impact on its perception. Chen et al. [8] believe that the effect of algorithmic management is different also due to the way it is used – from extremely strong control to a supporting function of work processes and decision-making. It is this variability in its implementation and use that leads to the different attitudes and opinions of those working in organizations – people react and adapt differently [19].

In parallel with the purely organizational aspects of algorithmic management, within the EU we can also talk about a regulatory dimension. Migliora [9] adds another aspect to the discussion – regulatory changes in the EU related specifically to algorithmic management. The adoption of a specific act related to algorithmic

management provides clarity on the complexity of the phenomenon under study – from technological, through managerial, to social and legal levels.

In parallel with these studies, a significant number of authors examine the relationship between the implementation of artificial intelligence in various organizational processes and the achievement of rapid and competitive company growth. Shahzad et al. [10] study the impact of artificial intelligence on small high-tech companies. They comment that this type of companies AI to deal with risks and achieve faster growth. In reality, however, the positive effect depends on many factors – including available resources, data quality, the level of development of the organization itself, the quality of management decisions, including readiness for change. Researchers confirm the positive effect of the use of AI, but state that its effect is limited by the lack of capacity and high costs. Similar results are observed in other studies. Fontanelli et al. [11] also reach similar conclusions. They say that AI does not always lead to stable improvement, as some companies observe fluctuating results. They conclude that the results depend directly on the way AI is used – companies that develop it themselves do better than those that have a ready-made software solution.

Additional empirical studies confirm the impact of AI on various aspects of firm performance. Yu, Chen and Ren [12] examine the effectiveness of AI in terms of factors for rapid growth; Hernández-Lagos [13] focus on the transparency of AI and the impact on firm profits; Adams et al. [14] examine the effects that are achieved in relation to the use of AI in pricing; Xu et al. [15] comment that AI innovations have a very large effect on the competitiveness of the company; Chen et al. [16] add that the use of artificial intelligence improves the efficiency of supply chains, increasing profitability and reducing costs.

Some of the authors reach bolder conclusions. For example, Pastor-Merino et al. [17] strongly advocate the opinion that firms that use artificial intelligence achieve much better results, which are expressed in higher revenues and faster growth compared to those that do not use it. In addition, scientists specify that the deeper AI is implemented in their activities, the stronger the positive effect on their productivity and development.

III. METHODOLOGY

The purpose of this study is to determine the role of algorithmic management in achieving accelerated growth in fast-growing companies. The object of the study are fast-growing companies operating in economic sectors characterized by a high degree of technological innovation (ICT, IT sector; Outsourcing and High-tech services; Advanced Manufacturing, Fin-Tech and digital financial services; Biotechnologies and digital health, creative and culture industries). The subject of the study is related to determining the influence of algorithmic management as a mechanism related to accelerating the growth of these companies.

At the same time, the study is based on the following hypotheses:

H1: The application of algorithmic management has a positive effect on the growth rate of fast-growing companies operating in high-tech sectors of the economy;

H2: The influence of algorithmic management on the growth of fast-growing companies is mainly due to the increase in operational efficiency and optimization of resources.

In order to fulfil the main objective and to verify the objectives thus defined, the study relies on the following methodological framework.

TABLE 1 METHODOLOGICAL FRAMEWORK

N	Phase	Methods and instruments
1.	Theoretical positioning	Literature review; Conceptual analysis
2.	Defining Hypothesis	Deductive method
3.	Design of the Research	Quality research
4.	Collection of empirical data	Interview, purposive sampling
5.	Data analysis	Qualitative thematic analysis
6.	Results interpretation	Interpretive analysis
7.	Summary and conclusions	Synthesis and conclusion

Due to the specific focus of the study and the very nature of the problem under study, the report uses an empirical qualitative study. The choice of this method is due to the fact that algorithmic management is currently still being identified and developed as a relatively new management practice, the specifics of which are difficult to capture through standardized questionnaires typical of quantitative research. The empirical study, in turn, is aimed at identifying the specific practices through which algorithms support decision-making, coordinate activities, allocate resources and lead to an overall increase in the operational efficiency of the enterprise.

For the purposes of the study, the semi-structured interview method was used. In this case, it is structured into 7 main sections, through which it is aimed to collect in-depth information related to the specific enterprise and the specific point of view of the interviewee.

TABLE 2 LOGICAL FRAMEWORK OF SEMISTRUCTURED INTERVIEW

Thematic Section	Key questions/ guidelines (Hypothesis)
1. Profile of the company	In which sector does the organization operate? What is the growth rate in the last three years? What are the main drivers of growth? (H1)
2. Level of digitalization and data usage	To what extent do you use data in management? What systems/tools do you use? Are there automated solutions? (H2)
3. Elements of Algorithmic management	Are algorithms used in decision-making? In which functions (planning, control,

	evaluation)? To what extent are decisions automated? (H1; H2)
4. Impact on operational efficiency	How does efficiency change after implementation? Is there process optimization? Are costs/time reduced? (H2)
5. Impact on growth	Does algorithmic management affect growth? In what way (scaling, speed, new markets)? (H1)
6. Organizational capabilities for data integration	How is data integrated into management? Is there process adaptation? How is analytics used for decisions? (H2)
7. Limitations and challenges	What difficulties do you encounter? - Are there any limitations to implementation? - What slows down the effect? (H1; H2)

The participants in the study were selected purposefully, and they had to meet several conditions at the same time: to be in an expert or managerial position (regardless of whether at the operational, middle, senior or executive management level), to work in companies where there are signs of intensive digitalization, use of data in management and a strategic orientation for accelerated development. The selection includes managers, owners, leaders of digital transformation teams, product managers, as well as experts working in an environment where algorithmic systems participate in the management process. These high requirements for the participants in the qualitative study are actually consistent with the need for the information to be obtained from individuals who have direct observations of the real functioning of algorithmic management in the organization.

The qualitative interviews were conducted at the beginning of the year, during the period January – March 2026 and covered a total of 12 participants. The analysis of the collected data was carried out using qualitative thematic analysis, based on a previously developed coding scheme. It includes the following thematic areas, which are in line with the research model – algorithmic management, operational efficiency, organizational growth, data work and dynamic capabilities. Within each theme, specific codes were defined, through which recurring semantic elements in the respondents' answers were identified.

IV. RESULTS

A. Results under H1: impact algorithmic management – accelerated growth

Within this hypothesis, the interaction between algorithmic management and accelerated growth of companies was investigated. Here, the goal was to determine whether respondents see the connection at all at first glance, how clear it seems to them and to what extent it is direct or rather mediated. As a result, most of the interview participants stated that they find a connection between algorithmic management and improved growth. On the other hand, however, they very rarely interpret it as a direct cause-and-effect relationship, but rather justify it as some form of accelerator, which, however, does not have the potential to be a source of growth in itself.

"I would not say that algorithms themselves make growth, but they definitely accelerate it." (R3)

"Without these systems, we would not be able to grow at this pace." (R7)

"They rather allow us not to suffocate when we grow." (R1)

Regarding the possibility of scaling the activity, the respondents mostly agree that algorithmic management leads to growth without leading to a linear increase in the resources used. That is, in terms of automation, we can say that it leads to scaling in a large part of the cases studied. Most respondents stated that thanks to automation they can work and take on contracts with more clients without having to increase the team responsible for servicing them. At the same time, automated processes, the presence of digital platforms and systems allow for the taking on of a greater volume of work, without this having a direct proportional impact on the resources necessary for the quality provision of this new volume of work.

- *"We managed to double the volume of work without increasing the team."* (R5)

- *"Algorithms allow us to process many more requests with the same people."* (R9)

- *"Scalability comes precisely from automation, otherwise we would have had to hire twice as many people."* (R2)

These opinions actually show that the growth achieved does not require more resources, but rather better information processing, carried out precisely through the use of algorithms.

Most of the interviewees commented that the introduction of algorithmic management in the organization reflects on several very important organizational elements. First of all, the organization becomes much more sensitive, flexible and adaptable to the changing demands of the market. That is, it not only receives feedback from its customers, but also has the opportunity to make decisions faster and implement activities, taking them into account. Next, many of the interviewees commented that the time for making management decisions has been shortened enormously, which significantly helps to increase the speed at which the organization develops. This in turn leads to the conclusion that growth is not only expressed in increased volume, but also in increased speed.

- *"We react in almost real time to the market."* (R8)

- *"Decisions that used to take days are now made in minutes."* (R4)

- *"Speed is what really changes the game."* (R6)

The conclusion that emerges from these observations and interview analyses is that algorithmic management leads to a reduction in decision-making time, which in turn leads to accelerated growth.

Expanding into new markets and reaching new customers is another very important aspect that interviewees acknowledge is achieved with algorithmic management. They state that with their help, much better targeting of new customers is achieved, as well as providing guidance for new segments and data-driven expansion. This leads to the conclusion that algorithmic management supports growth by achieving better information and reducing risk.

- *"We enter new markets much more confidently because we have data."* (R10)

- *"Algorithms show us where there is potential."* (R6)

- *"We reach new customers more easily."* (R11)

Some of the interviewees mentioned another aspect in which the supporting function of algorithms is clearly distinguishable – ensuring growth that is not accompanied by the so-called organizational overload. Very often, rapid development is accompanied by organizational chaos due to extremely rapid growth, while from a purely managerial perspective this leads to the risk of uncoordinated decisions and the possibility of chaos due to rapid growth. With algorithmic management, this growth becomes positively controllable. These observations lead to the conclusion that algorithms have the potential to play the role of a stabilizer in the accelerated growth necessary to ensure a smooth transition through the dynamic phases of growth.

- *"Without these systems, we would collapse organizationally."* (R1)

- *"Growth without automation leads to chaos."* (R8)

- *"Algorithms keep processes under control."* (R3)

However, not all interviewees see a strong positive effect of algorithmic management. Some of them admit that the importance of this type of management depends to a large extent on the context, the degree of digitalization and the organizational culture itself, on the relationships within the teams and with the management itself.

- *"If there is no quality data, algorithms do not help."* (R4)

- *"It is not a magic solution – you also need a good organization."* (R9)

- *"The effect depends on how they are used."* (R6)

From this point of view, the implementation of algorithmic management does not mean achieving automatic growth by itself. The capabilities of the organization and the specific environment in which it operates must be assessed very carefully.

As a result of everything considered so far, we can say that H1 is partially confirmed. Algorithmic management has an impact on achieving accelerated growth, but the interaction is not direct. It is more correct to say that algorithmic management has a mediated and amplifying accelerating effect on the fast development of companies. Therefore, algorithmic management is not a direct source of company growth, but acts as an accelerator, mediator and stabilizer of this growth. Its effect is mainly expressed in scalability, achieving better speed, better targeting and better control over processes.

B. Results under H2: impact algorithmic management – growth through effectiveness

Almost all interviewees admit that algorithmic management certainly leads to process optimization, which can be commented as its core mechanism. In fact, optimization through the use of algorithmic management can be achieved in several main ways - on the one hand, through automation of routine activities, which provide the opportunity for processes to be carried out effectively - using fewer resources, which in itself leads to fewer losses.

Next is the ability of algorithms to eliminate unnecessary steps, which in themselves do not lead to added value. Last but not least is the achievement of better coordination between the various operations, activities and processes performed in the organization. This in turn leads to the conclusion that algorithms provide smoother processes, thanks to which higher efficiency can be achieved, which in turn can lead to greater and faster growth.

“A large part of the routine tasks are now automated and this has made the work much easier.” (R7)

„Before, we had a lot of waiting between stages, now this has almost disappeared.” (R9)

“Coordination between teams has improved noticeably.” (R8)

“We have much better visibility into the processes and this improves coordination.” (R6)

The other main direction of improvement is related to the better allocation of resources, which is also recognized by most of the interviewees. Algorithms direct resources to where there is value, thus largely avoiding the risk of overspending. This also leads to better use of human resources and optimization of their time, including improved time to complete activities. The conclusion from this observation is related to the ability of algorithms, based on quality data, to make better decisions, related to better allocation of resources, which in turn also leads to improved effectiveness and even efficiency.

“We direct resources much more precisely to activities that bring value.” (R4)

“We now have clarity where it is worth investing time and effort.” (R10)

“The difference is that we now know where to put our efforts.” (R6)

“Algorithms save us a lot of wrong decisions.” (R1)

On the other hand, some of the interviewees directly commented that algorithmic management leads to a reduction in human errors. With more standardized processes and algorithmic decision-making, noise in the system is naturally minimized, which also contributes to improved final efficiency.

“We have definitely reduced errors, especially in daily tasks.” (R4)

“There are significantly fewer corrections, which saves us a lot of time.” (R7)

“Wastes have decreased because the processes are much more controlled.” (R2)

Observations and analysis from the interviews led to the categorical conclusions that algorithmic management leads to process optimization, better allocation of resources and the making of far fewer errors. From this perspective, algorithmic management is directly related to achieving improved operational efficiency, which will support the overall organizational development and growth of the company. In this sense, X2 is categorically confirmed. It should also be emphasized again that algorithms are not recognized as an indicator of rapid growth, but are in the conditions that support its emergence.

V. CONCLUSION

This study focuses on the relationship between algorithmic management and the achievement of accelerated growth of companies. The main conclusions of the study are related to the conclusions that algorithmic management does in fact have an impact on the growth achieved by the organization, but this impact is not direct, but mediated. Algorithms create the opportunity to improve operational efficiency - related to process improvement, better allocation of resources, making fewer mistakes when making routine decisions. They create conditions for achieving growth, but do not act as a mechanism for growth itself. In any case, however, the effect of algorithmic management is not automatic and depends on the business environment, the specific organizational culture, the level of digitalization and other specific contextual characteristics.

ACKNOWLEDGEMENTS

The publication is funded by the Bulgarian Scientific Fund, under Project N KP06H55/3 (“A conceptual model for evaluation of fast-growing companies operating in innovation-intensive industries, based on Artificial Intelligence methods”)

REFERENCES

- [1] V. K.Nhan, T. T. Thu, Mapping the landscape of algorithmic management in gig economy: A bibliometric analysis, International Journal of Information Management Data Insights, Volume 6, Issue 1, 2026, 100402, ISSN 2667-0968, <https://doi.org/10.1016/j.ijime.2026.100402>.
- [2] P. Liu, L. Yuan, How algorithmic management enhances team resilience: The role of informal leadership emergence and algorithmic transparency, International Journal of Information Management, Volume 88, 2026, 103042, ISSN 0268-4012, <https://doi.org/10.1016/j.ijinfomgt.2026.103042>.
- [3] J. M. Moritz, L. Pomrehn, H. Steinmetz, M. C. Wehner, A meta-analysis on reactions to algorithmic decision-making in human resource management, Human Resource Management Review, Volume 36, Issue 2, 2026, 101135, ISSN 1053-4822, <https://doi.org/10.1016/j.hrmr.2026.101135>.
- [4] N. Hajiheydari, M. S. Delgosha, Staying or leaving? A person-centred view of algorithmic management and gig worker attrition, Journal of Business Research, Volume 210, 2026, 116092, ISSN 0148-2963, <https://doi.org/10.1016/j.jbusres.2026.116092>.
- [5] J. Zhao, T. A. Syed, Making sense of algorithms: Workers' coping strategies for algorithmic management on digital platforms, Technological Forecasting and Social Change, Volume 223, 2026, 124443, ISSN 0040-1625, <https://doi.org/10.1016/j.techfore.2025.124443>.
- [6] B. Jianu, I.P. Tussyadiah, G.Miller, The toll of resisting algorithmic management, International Journal of Contemporary Hospitality Management, Volume 37, Issue 12, 2025, Pages 4065-4083, ISSN 0959-6119, <https://doi.org/10.1108/IJCHM-12-2024-1821>.
- [7] W. Liu, H. Yang, S. Liu, Algorithmic platform management and risk-taking behavior among Chinese food delivery riders, iScience, Volume 28, Issue 12, 2025, 114244, ISSN 2589-0042, <https://doi.org/10.1016/j.isci.2025.114244>.
- [8] W. Chen, A. Li, C.Pan, T. Yu, A. Ali, Y. Sun, Algorithmic management in the workplace: A systematic review and topic modeling integration using BERTopic, International Journal of

- Information Management, Volume 86, 2026, 102994, ISSN 0268-4012, <https://doi.org/10.1016/j.ijinfomgt.2025.102994>.
- [9] G. Migliora, Platform work and algorithmic management: Protecting workers irrespectively of their employment status, Computer Law & Security Review, Volume 60, 2026, 106267, ISSN 2212-473X, <https://doi.org/10.1016/j.clsr.2026.106267>.
- [10] F. Shahzad, M. T. Hoque, I. S. Khan, A. Arslan, AI for the underdogs: Navigating risk and growth in high-tech micro-firms through generative artificial intelligence, Journal of Strategy & Innovation, Volume 37, Issue 1, 2026, 200566, ISSN 3050-7901, <https://doi.org/10.1016/j.jsinno.2026.200566>.
- [11] L. Fontanelli, M. Guerini, R. Miniaci, A. Secchi, Predictive AI and productivity growth dynamics: Evidence from French firms, Journal of Economic Behavior & Organization, Volume 240, 2025, 107336, ISSN 0167-2681, <https://doi.org/10.1016/j.jebo.2025.107336>.
- [12] X. Yu, K. Chen, Z. Ren, Building the efficiency bridge: Artificial intelligence innovation, high-growth firms and industry competition through governance, Journal of Innovation & Knowledge, Volume 14, 2026, 100961, ISSN 2444-569X, <https://doi.org/10.1016/j.jik.2026.100961>.
- [13] P. Hernández-Lagos, The transparency of AI and the profits of the firm, Journal of Corporate Finance, Volume 99, 2026, 103002, ISSN 0929-1199, <https://doi.org/10.1016/j.jcorpfin.2026.103002>.
- [14] J. J. Adams, M. Fang, Z. Liu, Y. Wang, The rise of AI pricing: Trends, driving forces, and implications for firm performance, Journal of Monetary Economics, Volume 157, 2026, 103875, ISSN 0304-3932, <https://doi.org/10.1016/j.jmoneco.2025.103875>.
- [15] J. Xu, B. Zhang, H. Li, J. Lu, Y. Yu, From optimization to disruption: The role of AI-driven innovation in shaping firms' market competitiveness, Journal of Engineering and Technology Management, Volume 80, 2026, 101962, ISSN 0923-4748, <https://doi.org/10.1016/j.jengtecman.2026.101962>.
- [16] J. Chen, J. Bai, N. Mirza, M. Umar, Investing in intelligence: The impact of AI adoption and investment intensity on supply chain efficiency of green firms, Technological Forecasting and Social Change, Volume 227, 2026, 124631, ISSN 0040-1625, <https://doi.org/10.1016/j.techfore.2026.124631>.
- [17] A. Pastor-Merino, X. Martínez-Barbero, M. R. Vicente, J. Domenech, Does AI boost firm productivity? A web scraping and LLMs approach, Telecommunications Policy, Volume 50, Issue 2, 2026, 103138, ISSN 0308-5961, <https://doi.org/10.1016/j.telpol.2025.103138>.
- [18] K. Luchkov, G. Chipriyanova, M. Chipriyanov, (2025). Implementing Innovative Strategies for Competitiveness in the Era of Digital Transformation. In: Alzoubi, H.M., Cheng Ling, T., El Khatib, M. (eds) Innovative Dynamics in Management and Engineering (IDME) . ISCME 2024. Advances in Science, Technology & Innovation. Springer, Cham. https://doi.org/10.1007/978-3-031-90131-7_29
- [19] G. Chipriyanova, M. Chipriyanov, K. Luchkov, Investigation and Analysis of Attitudes Towards the Implementation of Artificial Intelligence in Internal Business Processes. In: Proceedings of the 15th International Scientific and Practical Conference "Environment, Technology and Resources", Rezekne, 2024, Vol. II, pp. 61–67. <https://doi.org/10.17770/etr2024vol2.8032>
- [20] T. Stoyanova, A., Koev, S. R., Stoyanov, P. P., Zhyvko, Z., & Laptiev, V. (2019). Strategic management of the personnel development of industry companies. Academy of Strategic Management Journal, 18(3).
- [21] V. Zinoviev, D. Koeva, P. Tsankov, R. Kutkarska, Review of Artificial Intelligence Applications in the Digital Energy and Renewable Energy Infrastructures. Energies 2026, 19, 1250. <https://doi.org/10.3390/en19051250>

Internal Fire Hydrants in Residential and Public Buildings as a Fire-Risk Mitigation Measure

Svilena Arabadzhieva

Faculty of Fire Safety and Civil Protection

Academy of the Ministry of Interior

Sofia, Bulgaria

ORCID [0000-0003-3339-2947](https://orcid.org/0000-0003-3339-2947)

Abstract— Internal fire hydrants (IFHs) are an active measure for initial fire suppression and for supporting firefighting operations by providing immediately accessible water within the building. This paper integrates a regulatory analysis, processing of statistics for 43,127 registered fires in public and residential buildings during 2015-2025, an analysis of 66 registered fires in 2015-2024 in which an IFH was used, data from thematic inspections of 2,203 high-rise residential buildings, and a parameterized event tree for evaluating the weighted contribution of IFHs to fire-risk reduction. The analysis shows that the current regulatory framework in Bulgaria imposes measurable requirements for coverage, flow rate, pressure, minimum water-supply duration, and maintenance. Of the 66 incidents analyzed, 63 (95.5%) involved an IFH reported as operational, yet inspections of the building stock reveal a widespread presence of latent deficiencies - missing equipment, lack of maintenance, and missing signage. This confirms that the actual risk-reduction effect of IFHs depends simultaneously on their regulatory provision, technical readiness, and the human factor. Primary numerical results from the questionnaire surveys and experiments are not available in the uploaded files; therefore, the paper shows how these data enter the model without introducing unsupported values.

Keywords— *internal fire hydrants; building firefighting water-supply installations; fire risk; event tree; reliability; maintenance; residential and public buildings.*

I. INTRODUCTION

Internal fire hydrants (IFHs) are a component of building firefighting water-supply installations intended to provide immediate access to water for first intervention and/or to support the actions of fire-service crews. In the international engineering framework, these systems are treated as active barriers whose contribution depends on adequate water delivery, reliability, and readiness for use [1]-[9]. EN 671-1 and EN 671-2 explicitly define hose systems as intended for use by occupants, whereas EN 671-3 places emphasis on maintenance so that the systems can

guarantee an initial emergency intervention for fire extinguishment [3]-[5].

In the Bulgarian regulatory system, the technical requirements for building firefighting water-supply installations (BFWSIs) with IFHs are governed primarily by Ordinance No. Iz-1971, whereas operational requirements are governed by Ordinance No. 8121z-647. From the perspective of fire-risk assessment, the decisive question is not merely whether an IFH is installed, but whether it is required by the code, whether it is operational, and whether it is actually used at a sufficiently early stage of fire development [1], [2]. Early water application is critical for limiting consequences, a finding also confirmed by large-scale experimental studies of firefighting operations published by NIST and FSRI [10], [11].

This paper combines a regulatory analysis, processing of the provided statistical files, results from thematic inspections, and a developed event tree through which IFHs are formalized as a fire-risk mitigation measure. The approach is parametric: instead of introducing fictitious estimates, the model shows how the different data groups are linked to branch probabilities and expected consequences.

II. AIM, DATA AND METHODS

The aim of the paper is to assess internal fire hydrants in residential and public buildings as a fire-risk mitigation measure through an integrated analysis of: (i) the current regulatory requirements; (ii) the registered fires in which an IFH was used; (iii) data from thematic inspections of the building stock; and (iv) a mathematical model of the alternative outcomes after fire occurrence.

The empirical part uses data from the General Directorate Fire Safety and Civil Protection of the Ministry of Interior, systematized by the author into three groups: summary statistics for fires in public and residential buildings for the period 2015-2025; fires in which an IFH was used; and results from thematic inspections of high-

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.152>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

rise residential and public buildings. Data from questionnaire surveys conducted among the population were also used.

The statistical analysis includes descriptive indicators, relative shares, and Wilson confidence intervals for key proportions. The logical structure is organized as an event tree (Event Tree Analysis, ETA), which makes it possible to trace all relevant outcomes after the initiating event and to determine the contribution of each barrier to the reduction of expected consequences [9].

An important limitation is the lack of data on how many of all registered fires occurred in buildings equipped with IFHs. For that reason, the ratio N_{used} / N_{fires} does not represent the conditional effectiveness of IFHs, but only a joint estimate of presence, operability, and actual use during fire. The primary numerical results from the questionnaire and experimental studies mentioned in the working materials are also unavailable; therefore, they are treated here as model parameters without introducing unsupported values.

III. REGULATORY REQUIREMENTS IN THE REPUBLIC OF BULGARIA

The current Ordinance No. Iz-1971 does not require BFWIS with IFHs for buildings in subclasses F1.3 and F1.4 with a maximum height of human occupancy up to and including 25 m, nor for buildings or parts of buildings in groups F1-F4 (except F1.3 and F1.4) with a volume up to 5,000 m³. For buildings outside these exemptions the requirement is triggered, and for buildings with a maximum height of human occupancy above 25 m in groups II-IV the installation must be looped (closed) [1]. This means that the presence of IFHs is normatively determined by the building's functional purpose, volume, and height.

The Ordinance also imposes measurable engineering criteria: fire hydrants are to be located at accessible places near entrances, corridors, and foyers; all rooms must fall within the reach of the compact jet; the minimum radius of the compact jet is at least 6 m; the required flow rates and the number of simultaneously operating hydrants are determined by tabulated requirements; and the water quantity must be ensured for at least 1 h. Where automatic water-based fire-extinguishing installations are present, simultaneity of water demand is also taken into account [1], [3], [4].

At the operational level, Ordinance No. 8121z-647 requires fire hydrants to be maintained in accordance with the manufacturer's operating instructions and BDS EN 671-3, with maintenance carried out by persons and traders authorized under the Ministry of Interior Act [2], [5]. Within the framework of state fire control, the procedure and conditions for inspections of facilities are regulated by Ordinance No. 8121z-882 [12].

The historical review in the working materials provided shows a substantial evolution of the threshold for residential buildings: no requirement in 1951-1956; a requirement for all buildings above 5 storeys in 1956-1959; above 6 floors in 1959-1963; withdrawal of the

requirement in 1963-1972; reinstatement for buildings above 10 floors in 1972-1978; a criterion of above 10 storeys or 30 m in 1978-2009; above 28 m in 2009-2025; and the current threshold of above 25 m from 2025 onward. In this sense, high-rise residential buildings constitute the most clearly identified class of facilities for which IFHs have both regulatory and operational significance.

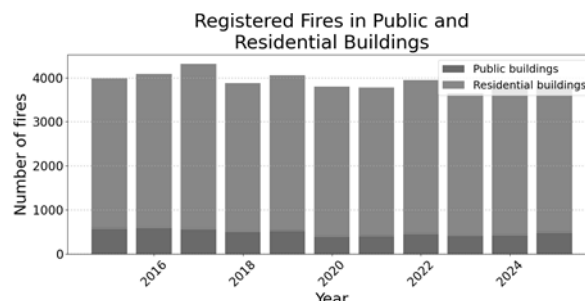


Fig. 1. Registered fires in public and residential buildings by year (2015-2025); author's processing of the uploaded fire-statistics dataset.

A. Total Number of Fires in the Building Categories Considered

During 2015-2025, a total of 43,127 fires were registered in the public and residential building categories considered, of which 5,237 were in public buildings and 37,890 in residential buildings. Residential buildings account for approximately 87.9% of all registered fires within this scope, which explains why the absolute number of cases in which an IFH was used is also higher for this category.

B. Fires in Which an IFH Was Used

A total of 66 fires were identified in 2015-2024 in which use of an IFH was recorded: 44 in residential buildings and 22 in public buildings. By year, there is no monotonic trend; a local maximum is observed in 2017 (11 cases), and a minimum in 2021 (3 cases).

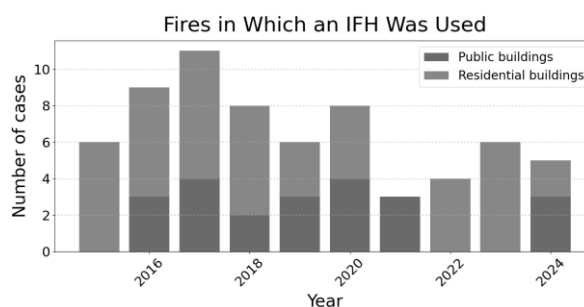


Fig. 2. Fires in which an IFH was used, by year and building type (2015-2024); author's processing of the uploaded datasets on IFH use in public and residential buildings.

In these 66 cases, IFHs were used by firefighters in 60 cases (90.9%) and by on-site persons - occupants or staff - in 6 cases (9.1%). For public buildings the ratio is 21 to 1, and for residential buildings 39 to 5. The reported operability of the IFH used was $63/66 = 95.5\%$; the 95% Wilson confidence interval is 87.5-98.4%. It is important to emphasize, however, that this share describes only the

cases in which there was actual demand for or use of an IFH, not the condition of the entire building stock.

Among residential buildings, 27 of the 44 cases (61.4%) were marked as high-rise buildings. Floor information is available for 36 cases, and 18 of them (50.0%) occurred on the 11th floor or higher. This supports the engineering relevance of IFHs in conditions of vertical building development, where pressure deficit with height and the time needed to reach the seat of fire become more critical.

When related to all registered fires in public and residential buildings over the same period, the cases in which an IFH was used amount to 0.168% overall, 0.462% for public buildings, and 0.127% for residential buildings. These values are not an estimate of IFH effectiveness, because the denominator does not contain information on whether an IFH was actually present in the building. Formally, the observed share is closer to $P(\text{IFH used} \cap \text{IFH operable} \cap \text{IFH present} | \text{fire})$ than to $P(\text{IFH used} | \text{IFH present and operable, fire})$.

In public buildings, the largest number of cases involving IFH use was recorded in accommodation and food service activities (10), followed by public administration (4) and education (3), which may be explained both by the characteristics of the building stock and by the presence of staff on site.

C. Inspections and Latent Failures

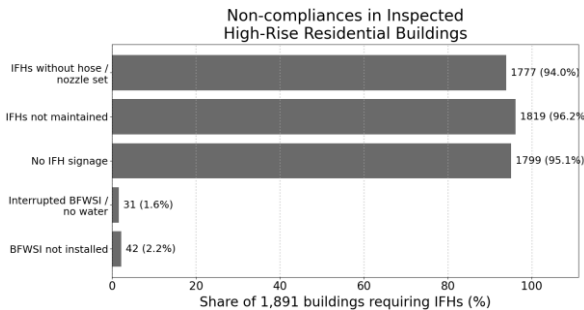


Fig. 3. Non-compliances identified in inspected high-rise residential buildings; shares are calculated relative to the 1,891 buildings in which IFHs were required; author's processing of the uploaded thematic-inspection dataset.

Among the 1,891 buildings in which IFHs were required, 1,777 IFHs lacking hoses or nozzles were recorded (94.0%), 1,819 IFHs not maintained (96.2%), 31 cases of interrupted BFWSI or lack of water (1.6%), 42 cases of a BFWSI not installed in violation of construction rules (2.2%), and 1,799 cases with no IFH signage (95.1%).

Inspection of 187 high-rise public buildings established that IFHs were required in all facilities and that there were no cases of a missing BFWSI. Violations were found in 17 facilities: 5 IFHs lacking equipment, 15 not maintained, 1 interrupted BFWSI/no water, and 15 without signage.

At first glance, the high reported operability in real incidents and the massive deficiencies identified by inspections appear contradictory. In fact, however, they describe different conditional sets. The list of 66 fires contains cases in which an IFH had already been sought or used, whereas the inspections describe the condition of the available building stock before a fire occurred. Consequently, the inspections reveal latent failures that may break the barrier before it is ever activated.

IV. EVENT TREE AND MATHEMATICAL MODEL

ETA is an inductive procedure that considers all possible outcomes after an initiating event, taking into account whether the protective barriers function or fail [9]. For the purposes of this paper, the initiating event is F_0 - occurrence of a fire in a residential or public building - and the relevant barriers are: normative presence of a BFWSI with IFHs, technical operability, actual tactical choice of use, and the human factor among occupants.

The full event tree was developed in a separate working file, and Fig. 4 presents the event-tree logic used in the mathematical model.

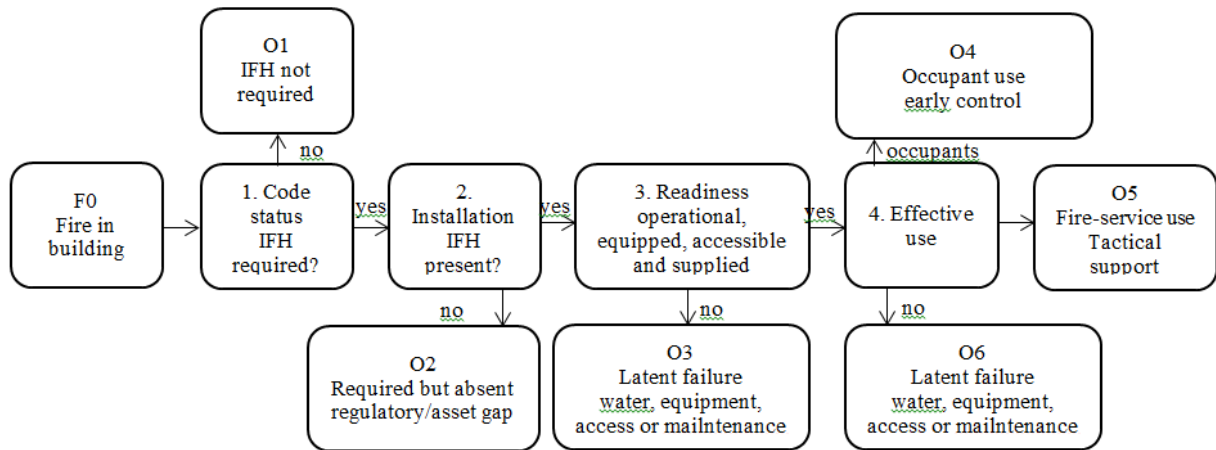


Fig. 4. Simplified event tree for internal fire hydrants used in the generalized model

TABLE I. MAIN PARAMETERS USED IN THE GENERALIZED EVENT-TREE MODEL

Parameter	Meaning and primary data source
pREQ	IFH required by code for the building/fire case; regulatory classification and building-stock data.
pINS	Required IFH physically installed; inspections, commissioning and asset records.
pRDY	Installed IFH operational, equipped, accessible and supplied; functional inspections and maintenance records.
pO, pG, pN	Use by occupants, by fire service, or no effective use; fire-incident reports, drills and surveys.
pC, pT	Correct/timely occupant action and tactical fire-service use; training records, experiments and incident narratives.
Lk, etak	Loss and loss-reduction factor for terminal state Ok; incident outcomes, expert calibration and simulations.

The generalized model is written at the level of the initiating fire event F0. It separates three different questions that should not be merged statistically: whether an IFH is required and installed, whether it is ready at the moment of demand, and whether it is used early enough to reduce consequences. Table I summarizes the main parameters. This separation prevents the 66 recorded use cases from being interpreted as a direct measure of effectiveness for the whole building stock.

The terminal states of the simplified tree are: O1 - IFH not required; O2 - required but absent; O3 - installed but not ready; O4 - early occupant use; O5 - fire-service use; and O6 - no effective or timely use. With $pO+pG+pN=1$, the branch probabilities can be written as:

$$P\left(\frac{O1}{F0}\right) = 1 - p_{REQ} \quad (1)$$

$$P\left(\frac{O2}{F0}\right) = p_{REQ} \cdot (1 - p_{INS}) \quad (2)$$

$$P\left(\frac{O3}{F0}\right) = p_{REQ} \cdot p_{INS} \cdot (1 - p_{RDY}) \quad (3)$$

$$P\left(\frac{O4}{F0}\right) = p_{REQ} \cdot p_{INS} \cdot p_{RDY} \cdot pO \cdot pC \quad (4)$$

$$P\left(\frac{O5}{F0}\right) = p_{REQ} \cdot p_{INS} \cdot p_{RDY} \cdot pG \cdot pT \quad (5)$$

$$P\left(\frac{O6}{F0}\right) = p_{REQ} \cdot p_{INS} \cdot p_{RDY} \cdot (1 - pO \cdot pC - pG \cdot pT) \quad (6)$$

The failure causes observed during inspections are attached to the readiness branch. If q_j is the conditional probability of failure cause j when an installed IFH is not ready, then:

$$\sum q_j = 1 \quad (7)$$

$$j \in \{\text{water/pressure, equipment, access/signage, maintenance}\}$$

Thus, missing hoses/nozzles, lack of maintenance, inaccessible cabinets, missing signage, and pressure or water-supply problems do not make the event tree more complicated; they explain how the readiness probability pRDY should be estimated and improved.

If Lk is the expected loss for terminal state Ok and R0 is the reference risk without IFH contribution, the expected risk with IFHs is:

$$RIFH = P_{(F0)} \cdot \sum_{k=1}^6 P_{\frac{Ok}{F0}} \cdot L_k \quad (8)$$

The weighted contribution of IFHs as a risk-mitigation measure is expressed as the relative reduction of risk:

$$WTFH = \frac{R0 - RIFH}{R0} \quad (9)$$

Equivalently, when $Lk = L0 \cdot (1 - etak)$, where etak is the fractional loss reduction in terminal state Ok, the contribution can be interpreted as a probability-weighted sum of the reductions achieved by the terminal branches:

$$WIFH = \sum_{k=1}^6 P_{\frac{Ok}{F0}} \cdot \eta_k \quad (10)$$

The human-factor terms are estimated separately from technical readiness. For example, pC may be estimated as the share of respondents or trained occupants who describe the correct and safe sequence of actions, while time-to-water application can be compared with a critical threshold τ_{crit} . The important modeling rule is that survey and drill results populate pC and pO; they do not substitute for measured pRDY.

This form is deliberately compact. It can be populated with available national statistics, building inspections, maintenance records, fire-incident data, occupant surveys and drill results, while preserving the distinction between code compliance, technical availability and actual use. Reliability and maintainability concepts remain important because hidden failures are revealed only when the system is inspected or demanded [12], [13].

V. DISCUSSION

The revised event tree highlights that IFHs reduce fire risk only when four barriers work in sequence: the system is required for the building, it is physically present, it is technically ready, and it is used at a stage when water application can still influence fire development. This interpretation is more useful for practice than a single effectiveness percentage, because each branch corresponds to a concrete management action.

The high reported operability in the 66 fires with IFH use should therefore be interpreted with caution. These cases are conditioned on the fact that the IFH was already found, selected and used. They cannot be generalized to all fires in buildings where an IFH may have been absent,

inaccessible, incomplete, unmaintained or not considered by occupants. The inspection results are essential because they describe latent failures before demand, which is the critical point for a hidden protection system.

For inspections, the practical implication is to move beyond a visual check of the cabinet. A risk-based inspection protocol should include: verification that an IFH is required for the building; confirmation that the installation is present and accessible; control of hose, nozzle and handwheel completeness; inspection of cabinet signage and opening; review of maintenance documentation; and functional pressure/flow testing at the hydraulically most unfavorable point. High-rise residential buildings should be prioritized because vertical development increases the importance of pressure, access time and tactical support.

For maintenance, the model shows that the most efficient interventions are those that increase pRDY. Missing hoses and nozzles, unmarked cabinets and overdue maintenance are not minor administrative issues; they move the fire into a branch with no effective IFH contribution. Building managers should keep a simple register containing the location of each cabinet, date of last inspection, identified defects, corrective action, contractor, and next due date. Tamper-evident seals, standardized spare equipment and clear responsibilities for monthly visual checks can reduce repeated deficiencies.

For occupants and staff, the results point to a different intervention: increasing pO and pC without compromising evacuation safety. Training should be short, practical and limited to safe first actions: recognizing the cabinet, calling the fire service, avoiding smoke exposure, using the hose only for incipient fires when an escape route remains available, and stopping use when conditions become unsafe. In public buildings with staff on site, annual familiarization and short drills are justified. In residential buildings, information boards, instructions inside the cabinet and building-manager briefings are more realistic than complex drills for all occupants.

For fire-service operations, IFHs appear to be especially relevant as a tactical support measure. In the analyzed residential cases, the system was used mainly by fire-service crews rather than by occupants. This means that design and maintenance should support professional use: unobstructed access to cabinets, predictable location, reliable pressure at height, looped installations where required, and information about the installation available to responding crews.

For reporting, the current data structure is the main barrier to a stronger quantitative assessment. Future fire-incident forms should include fields for: whether an IFH was required; whether it was present; whether it was operational and complete; who used it; whether water, pressure or access problems occurred; approximate time to water application; and whether IFH use affected localization, spread, casualties or material loss. These fields would allow direct estimation of P(successful use |

IFH present and ready, fire), rather than relying on indirect ratios.

Finally, the model can support prioritization. Branch O2 identifies regulatory or asset gaps; O3 identifies maintenance and readiness problems; O4 and O5 identify successful use; and O6 identifies cases where a present system did not influence the outcome. Reporting the share of inspections or incidents in each branch would give authorities and building owners a simple set of performance indicators. This is consistent with broader fire-safety assessment practice, where the value of a protective measure depends on both technical reliability and organizational readiness [14].

VI. CONCLUSION

1) The regulatory framework in the Republic of Bulgaria sets engineering-measurable requirements for BFWsIs with IFHs - concerning presence in specific building classes, location, coverage, flow rate, pressure, simultaneity and minimum water-supply duration [1]-[3], [8], [9].

2) The statistical files provided include 43,127 registered fires (2015-2025) and 66 cases (2015-2024) in which IFH use was recorded. The 63 operational IFHs among these 66 cases (95.5%) describe only recorded use cases and should not be interpreted as the readiness of the entire building stock.

3) The thematic inspections show substantial latent deficiencies - missing equipment, lack of maintenance and missing signage. These findings directly affect the readiness probability pRDY and are therefore central to the actual risk-reduction effect of IFHs.

4) The simplified event tree and generalized mathematical model express IFHs as a sequence of barriers: requirement, presence, readiness and timely use. The model is easier to reproduce because failure causes are handled as diagnostics of the readiness branch rather than as numerous terminal states.

5) The most immediate practical measures are stricter functional inspections, restoration of missing equipment, visible and standardized signage, clear maintenance registers, short occupant or staff instructions, and better integration of IFHs into fire-service tactical planning.

6) A more complete quantitative assessment requires improved incident reporting. Future records should capture IFH requirement, presence, condition, user type, time to water application, technical problems and observed effect on fire development and losses.

REFERENCES

- [1] BDS EN 671-1:2001, Fixed firefighting systems - Hose reel systems with semi-rigid hose.
- [2] BDS EN 671-2:2012, Fixed firefighting systems - Hose systems with lay-flat hose.
- [3] BDS EN 671-3:2009, Fixed firefighting systems - Hose systems - Part 3: Maintenance.
- [4] NFPA 14: Standard for the Installation of Standpipe and Hose Systems.

- [5] NFPA 25: Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems.
- [6] ISO 16732-1:2012, Fire safety engineering - Fire risk assessment - Part 1: General.
- [7] M. Rausand, Chapter 3: Event Tree Analysis. Norwegian University of Science and Technology. [Online]. Available: <https://www.ntnu.edu/documents/624876/1277590549/chapt03-eta.pdf/6f3e1b19-4824-4812-adc8-9762d2201c22>, 20.03.2026, (Accessed April 18, 2026)
- [8] Ordinance No. Iz-1971 of 29 October 2009 on the construction-technical rules and norms for ensuring fire safety. [Online]. Available: <https://lex.bg/laws/ldoc/2135653786>, (Accessed April 06, 2026)
- [9] Ordinance No. 8121z-647 of 1 October 2014 on the rules and norms for fire safety during the operation of facilities. [Online]. Available: <https://lex.bg/laws/ldoc/2136357759>, (Accessed April 07, 2026)
- [10] J. Averill, L. Moore-Merrell, A. Barowy, R. Santos, R. Peacock, K. Notarianni, and D. Wissoker. (2011). Report on Residential Fireground Field Experiments. International Fire Service Journal of Leadership and Management. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909096 (Accessed April 27, 2026)
- [11] R. Zevotek, K. Stakes and J. Willi, Impact of Fire Attack Utilizing Interior and Exterior Streams on Firefighter Safety and Occupant Survival: Full-Scale Experiments. <https://dx.doi.org/10.54206/102376/DNYQ2164>
- [12] Ordinance No. 8121z-882 of 25 November 2014 on the procedure and conditions for the implementation of state fire control. [Online]. Available: <https://www.lex.bg/bg/laws/ldoc/2136396531>, (Accessed April 05, 2026)
- [13] H. Boyd and C. LoCurto, Reliability and Maintainability for Fire Protection Systems. Fire Safety Science, vol. 1, pp. 963-970, 1986. [Online]. Available: <https://publications.iafss.org/publications/fss/1/963>, (Accessed April 17, 2026)
- [14] S. Parvanov, Challenges to the assessment of fire safety and protection in fires, disasters, and emergency situations in facilities. In: Proceedings of the Jubilee International Scientific Conference '50 Years of Higher Education at the Academy of the Ministry of Interior', Part Two. (2019). Sofia, pp. 178-182. [in Bulgarian].

Two Approaches to Seeking Public Support in Addressing Challenges in the Field of International Security

Plamen Atanasov

Faculty of Secure and Defence
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
paatanasov@nvu.bg

Abstract— In the contemporary field of international affairs, China's economic, geopolitical, and military rise is a significant challenge. The focus of this study falls on the response which these circumstances find in the context of national security in two states of established economic and geopolitical standing. In this scientific framework, international security is situated as the object of the study. The subject of the research is the complex of activities undertaken by governments to build transparency in the public space about their international affairs. The aim of the study is to explore a discovered approach for overcoming the latency of the public opinion, relative to China's rise. Presented are two principally different policies, which were implemented in the USA and in Russia, in response to the challenge of 'China's rise'. The research uses the progress of digital technology, and on this ground realizes a phenomenological approach which implements methods in the field of Science for communications, Public diplomacy, and Comparison of open-source data. This whole complex is united in the context of security in an international environment. The important part of the result of this study is the quantitative description of certain social dependencies that are essential for national security. These dependencies are perceptible to people yet inherently challenging to measure.

Keywords— China's rise, external security, media content, public opinion

I. INTRODUCTION

It is a widely known fact that society is a key factor for a country's vitality. Therefore, the process of shaping a unified public opinion is of interest to scientists and experts in the field of Security. It is obvious that if the public sentiments are negative, the success of one executive power's initiative is impossible. Because of this, in the country activities are arranged to attract the public support for the government's initiatives and for the positioning specific questions far from the focus of the public opinion. Due to their complexity and multi-directionality, the

vectors in which the public activity is shaping are difficult to describe. The reason is that the empirical testing of this kind activity is relevant for science. Even more interesting is the algorithm through which these mechanisms are realised. The work shows a quantitative description of such process and a bond between public interest and the presence of information in the media. The discourse does not primarily address media freedom; instead, it examines the interplay between governmental security policy objectives, media content and the construction of public opinion. The objective is to demonstrate, through an analysis of two diametrically opposed approaches to the same challenge, that the shaping of society constitutes one indispensable factor in security policy. In this context, the work does not examine the media themselves, but rather the consequences that the manner of presenting information about a given challenge has in relation to governmental security policies. An example has been shown of a difference in the picture offered for public perception in the USA and in the RF; however, the identified mechanism is universal and can manifest in various states, under varying circumstances, in accordance with which state authorities seek a particular kind of support for their policies in the field of security.

For the sake of specificity, working definitions have been introduced in the paper. According to them:

- public opinion is understood as a complex, synergistically acting aggregate of expectations, attitudes, preferences, and perceptions of reality that are shared within society and determine its readiness to act in a particular direction;
- public support is the understanding, approval, and above all willingness to cooperate that have been agreed upon within society and around which any potential social activity is united;

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.130>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

– public attention is explained by the "list" of topics on which people focus. It is understood as a key factor in the formation of the public agenda. It also contains a negative element, in that due to a lack of attention, society may lower its critical barriers toward other topics that are important for security.

It is a widely acknowledged fact in academia that the media do not reflect everything that occurs, and in this way media coverage is capable of influencing public opinion and public support.

II. MATERIALS AND METHODS

The exploration of the challenge is based on a phenomenological approach; i.e. the facts are explored through the way they are processed by the human consciousness and the way they are thought of and talked about.[1] By its very nature, the approach lends itself more to the examination of qualitative factors than to the empirical presentation of observed dependencies. For this reason, it is used in the social sciences, including in the study of security, insofar as security is a social construct.

On the one hand, such approach corresponds to the understanding of security, defined by the Copenhagen School. According to it, security is a social construct, and relevant events become challenges or threats only when they are perceived as such.[2] This framework justifies the application of the phenomenological approach in scientific research, especially when explored are matters relating to public stance, public opinion, and the manners for obtaining public support. The established connection with the concept of the Copenhagen School justifies the expectation that the phenomenological approach will become increasingly prominent in the field of Security. This element also corresponds to the relevance of matters, such as the one about working with the people in a country. On the other hand, among security experts it is widely spread that the engagement with the public opinions, expectations, and stance is key for the success of policies through which a country overcomes the challenges in its domestic and foreign security.[2] According to the renowned American researcher Harold Lasswell, the functions of communication are: 1. To organise the community - correlation; 2. To observe, reflect, and trace the changes in the environment – surveillance; 3. To pass knowledge through the years – transmission. [3] Lasswell's concept that a major function of communication (incl. the media content; author's note) is to organise the community towards one activity or another serves as a foundation of the statement that the media content (also referred to as media narrative in the present work) is a tool for modelling the type of the support that governments seek and receive for their policies. Whether and to what extent governments utilise this tool is complex matter which is unlikely to be possible to explore fully. We cannot claim definitively when governments use this tool – a state, typical for the fields of Social science and, respectively, for the one of

Security (according to the Copenhagen School of security studies).

On the one hand, such approach corresponds to the understanding of security, defined by the Copenhagen School. According to it, security is a social construct, and relevant events become challenges or threats only when they are perceived as such.[2] This framework justifies the application of the phenomenological approach in scientific research, especially when explored are matters relating to public stance, public opinion, and the manners for obtaining public support. The established connection with the concept of Copenhagen School justifies the expectation that the phenomenological approach will become increasingly prominent in the field of Security. This element also corresponds to the relevance of matters, such as the one about working with the people in a country. On the other hand, among security experts it is widely spread that the engagement with the public opinions, expectations, and stance is key for the success of policies through which a country overcomes the challenges in its domestic and foreign security.[2] According to the renowned American researcher Harold Lasswell, the functions of communication are: 1. To organise the community - 'correlation'; 2. To observe, reflect, and trace the changes in the environment – surveillance; 3. To pass knowledge through the years – transmission. [3] Lasswell's concept that a major function of communication (incl. the media content; author's note) is to organise the community towards one activity or another serves as a foundation of the statement that the media content (also referred to as media narrative in the present work) is a tool for modelling the type of the support that governments seek and receive for their policies. Whether and to what extent governments utilise this tool is complex matter which is unlikely to be possible to explore fully. We cannot claim definitively when governments use this tool – a state, typical for the fields of Social science and, respectively, for the one of Security (according to the Copenhagen School of security studies).

The phenomenological approach in the present study has been applied in the following methodological sequence: 1) to the extent possible, the challenge has been separated from conformist notions and from prior public emotions surrounding the issue; 2) attention has been directed toward the challenge of China's rise, and more specifically toward the way in which it is perceived - or rather, could be perceived - in the societies of Russia and the United States; 3) an intentional analysis has been carried out regarding how the challenge may be linked to public expectations and attitudes, as well as to state security policies; 4) the essence of the public experience has been sought - that is, an exposition of the expected public support upon the final outcome of policy in the field of international security. In this form, the methodology corresponds to theoretical frameworks developed by Smith, J. A., Flowers, P., & Larkin, M. [4]

The methodology presented highlights the obvious characteristic of the phenomenological approach – that it combines the objective and the subjective, the quantitative and the qualitative, into a complex unity. For this reason, the reproducibility of results is sought not so much through repetition of the experiment, but through replication of the findings reached. In this case, this is tied to the assertion that the public support for state policies in the field of security can be modelled through a specific combination of feeding information to the media and initiatives aimed at steering public activity in a particular direction. This does not mean that in the same or highly similar events occurring at a different time and place, the media will publish the same headlines. The way in which the phenomenological approach is understood in this paper is that there is a high probability of applying the same manner of modelling public support through directing information to the media and combining this process with accompanying initiatives by the state authorities.

This research uses the internet-based platform Google Trends (<https://trends.google.com>) as a tool for quantitative observation of the chronology of search queries across the web. The phrase “China's rise” was used as a search term for entire world. It describes one of the challenges to international security, which various scholars regard as a precondition for the emergence of a risk of conflict between a rising and an established power within the international security system (the Thucydides Trap). [5] Drawing on various theoretical frameworks (some of which have already been cited), as well as on the tangible political reality of the first half of the 2020s, China (as a rising power) and the United States and Russia (as established powers) are examined as such forces. The reason for selecting the United States and Russia is the events of the war in Ukraine and the visibly divergent directions in which the two states are organising their policies toward China.

The concept that the relationships between government and the public constitute a primary factor in state policy [6], and the recognition that this interaction is highly significant for security [7] directs scientific attention to the correlation between policy activity and media content during the period of August 2024 year.

The phrase China's rise is understood as an established term among researchers in the field of security, and when searching Google Trends, the side effects of translation — which could potentially exist across different countries — were not examined. This was done during searches on online platforms in the Russian Federation and in the United States. It was noted that in public media the language is more varied.

The search was conducted in the following sequence:

1) Using the Google search engine, materials in American media were searched. The search was carried out for a specific period (07.08.2024 – 17.09.2024). The restriction was applied via Google Tools – Custom range;

2) Since the search for the phrase “China” AND US media did not yield results (on the first three suggested pages, the results were dominated by media outlets such as YouTube, The Guardian, China Media Project, and similar), the search was further specified through a direct examination of individual media sources, under the same restrictions (for the same period) and using the following Google operators:

- “China's rise” site:cnn.com;
- “China's rise” site:wsj.com;
- “China's rise” site:tass.com

A check was also conducted using the word “China” through the following operators:

- “China” site:cnn.com;
- “China” site:wsj.com;
- “China” site:tass.com

- 3) For specificity, the results suggested by Google were verified as content within the websites of CNN, The Wall Street Journal, and TASS.

III. RESULTS

The research is focused on a challenge that overcomes the frame of interactions among the directly involved countries. The geopolitical situations of this kind - regardless of whether they involve active warfare or request for economic rearrangement - are of significant relevance to international security. Such conditions often constitute a prerequisite for crises and can trigger consequences for multiple countries that aren't directly engaged in the conflict. An emblematic example is the Iraq crisis of 2003 year, which influenced the security strategies all the way to the European Union [8]. Therein lies the Thucydides Trap for our contemporary age.

1) separation from conformist notions and prior public emotions surrounding the issue

It is evident that demands for economic realignment represent a challenge for states and the societies within them. A useful convenience for this study is that in politics there operates the rule formulated by the British statesman H. J. T. Palmerston: "We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow". [9] For this reason, the conformism and emotions that accumulate in society in response to a given challenge are not expected to be particularly lasting. This is why, in examining China's rise as a challenge in the United States and in the Russian Federation, any pre-existing layers of conformism and emotion are eliminated as unwanted confounding factors in the study. It is a widely known fact that until the early 1990s, China – despite being a country of enormous population – was not treated intensively as a competitor to the highly developed states.

Some of today's researchers in the field of security warn that Chinese policy is directed more inward than outward. For this reason, they argue that "the conventional view of China plays down the economic and diplomatic arenas that a war-fighting approach is unsuited to address." [10]

2) Focusing on the way in which China's rise is perceived – or rather, could be perceived – in the societies of the RF and the USA

The focus in this research is concentrated on the changes in the international economic and political environment to security, which are situated after the obvious China's rise over the past years. The rapid economic and technological growth during this period has led to an expansion of China's interests towards international trade routes; to the alternative's possibilities for the export of China's products and technologies; to the shaping the international relation, generating both attraction to and repulsion against China's foreign policy on world-wide important issues. Some countries perceive China's rise as an opportunity for friendship and cooperation. Other countries interpret this geopolitical development as a potential threat to both internal and external security. It is widely known that the USA government has expressed concerns regarding 5G technology, particularly due to its development and leadership by Chinese digital companies. The USA's policy is concerned also over the growth of Chinese industrial production, which is perceived as a potential threat to American industry and domestic markets. On the other hand, the Russian policy is widely characterized as oriented toward cooperation with China. There is no doubt that such policy orientations require public support to be sustainable. In accordance with contemporary theoretical frameworks, the media play a significant role in these supporting processes.[11]

3) intentional analysis of how the challenge can be connected with public expectations and stance, as well as with state security policies

A considerable number of authors also cover the view that 'security is no longer only a value but a state which is to be guaranteed by society through providing the necessary conditions'.[12] The scholarly position that government policies require public support can be understood as a socially oriented concept, linked to the framework, developed within the Copenhagen School of security studies.[13] It is generally assumed that such public support needs to be shaped through various forms of transparency, including in some cases through full media blackouts also. [14] This viewpoint on the contemporary international security environment directs the focus of this topic to the managing of public interests and public opinion in the USA and Russia (RF), as two countries, both of which are obviously recognized as some of the most

influential in foreign policy. The evolution of the war between Russia and Ukraine, and the active stance of the United States toward the conflict, dispel any doubts about the choice.

4) exposition of the expected public support towards the end result of the policy in the field of international security

The result suggests that the observed methods for shaping the synchronization between foreign policy activity and public support are positioned at opposite ends of the spectrum of possibilities.

The queries on the topic 'China's rise' across the web are presented on the Figure 1. It can be seen that, with the exception of brief periods of lull, queries reflecting interest in the topic are generated on the internet continuously, with a visibly increasing trend over the past year.

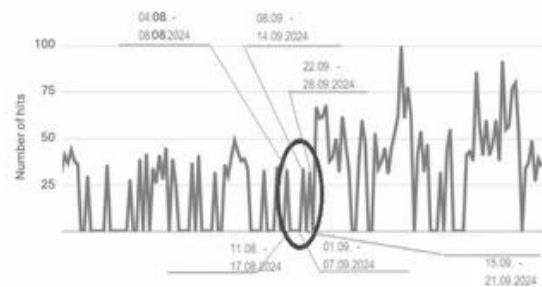


Fig. 1. Highlights (in a five-year period) a temporal interval during which no discernible activity is observed. (<https://trends.google.com/trends/explore?date=today%205-y&q=China's%20rise&hl=bg>)

In keeping with the phenomenological analysis, a compelling question arises as to what happens during such a period of lull and how information about these events (if any exist) is brought to the attention of society. For this reason, one such period of lull has been selected from the data shown in the graph covering the five-year period (2020–2025). It runs from 07 August to 17 September. This is indicated by the corresponding dates in Fig. 1.

During the period from 07th August 2024 to 17th September 2024, in which no significant web search is observed, several developments in Chinese foreign policy are of particular interest: 1) on the 19 of August a collision between Filipino and Chinese naval vessels was reported [15]; 2) the Prime minister of Vietnam conducted an official visit to China, contributing to further strategic cooperation between the two countries [16]; 3) China and Belarus conclude an agreement on economy and technological partnership [17]; 4) Chinese government actively develops a series of diplomatic visits, during which the questions about Russia-Ukraine conflict are discussed [18]; 5) For 4th to 6th September in Beijing was realized a major diplomatic forum with African states [19]; 6) Ahead of the UN General Assembly China calls for a reassessment

of the challenges facing contemporary multipolar world [20]. In summary, the situation facing that Chinese government: 1) is pursuing a diplomatic initiative to support its position on the Russia-Ukraine conflict and to reinforcing its orientation to cooperating with Russia; 2) is developing the activity aimed at strengthening involving with Africa countries; 3) is developing instrumental activity at other Asian countries; 4) ahead UN maintains its claim to an influential position in the contemporary multipolar world.

Further research in Google Trends revealed inconsistency in the data regarding queries generated from Russia. Due to a problem of a nature unknown to us, at the time of writing the paper, instead of the graph generated by the query for *China's rise* in March 2026, a check of the Google Trends platform in May displays the message "Oops! Something went wrong. Please try again in a bit." (<https://trends.google.com/trends/explore?date=today%205-y&geo=RU&q=China%27s%20rise&hl=en-GB>). Consequently, this result does not allow for reproducibility of the study. For this reason, the search has been continued in the direction of media content during the period marked in Fig. 1.

The observation over the media content regarding incidents from 07th August 2024 to 17th September 2024 (via search in Google and in the open media platforms) illustrates the differences in public interest regarding the topic 'China's rise'. Explanations for these variations have been examined through the analysis of media narratives in the RF and in the USA. One reason is that the publications from influential agencies are disseminated across multiple media platforms and achieve widespread diffusion on social networks. Accordingly, the moderation of instrumental action in the public sphere is conducted by influential media platforms.

As noted in the description of the methodology, the initial search for media publications using the query: "China" AND "US media" ([https://www.google.com/search?q=\"China\"+AND+US+media&sca_esv=fcd476843e4cb329&tbs=cdr:1,cd_min:8/7/2024,cd_max:9/19/2024,sbd:1&tbm=nws&ei=ykz_adgGN6Exc8Pq8ugwQs&start=20&sa=N&ved=2ahUKEwjfre2LvayUAxVeQvEDHasIKLg4ChDy0wN6BAGGEAc&biw=1870&bih=969&dpr=1](https://www.google.com/search?q=\)) did not produce the expected result. The outcome returned multiple pages, but they were not assessed as relevant for media influence or were not from American media outlets (despite the Google indication). Below are the first several indicated headlines:

How the EU risks falling further behind the US and China (DW News); *US-West* (China Media Project); *US thinktank leader arrested on charges of acting as unregistered agent of China* (The Guardian); *China warns students against 'beautiful women' and 'handsome guys' who might turn them into spies* (NBS News); *China says it is ending foreign adoptions, prompting concern from US* (The Guardian); *\$50 billion, a million jobs and a red carpet welcome: China woos Africa as U.S. struggles to keep up*

(NBS News); *South China Sea: Can the Philippines and US stop China?* News Desk (YouTube).

Obviously, these headlines are not relevant to the constraints of the scientific study, but they suggest that more active searching is directed toward sources other than American media (The Guardian, China Media Project, DW).

For this reason, a more specific search was conducted for the same period, restricted to media websites. The search results were as follows:

- "China's rise" site:cnn.com:

For CNN, Google provides numerous headlines; however, careful examination shows that it is difficult to identify the topic "China's rise" within them. Some of the first suggested headlines include:

China's one-child policy hangover: Scarred women dismiss ... (18.08.2024); *For decades, Chinese workers have retired relatively early. ...* (13.09.2024); *A dangerous new flashpoint is fast emerging in the South China Sea* (27.08.2024); *China-Africa ties 'best in history' claims Xi as Beijing* (05.09.2024); *China and Russia are ramping up joint military drills. ...* (17.09.2024); *China's secretive space plane has returned to Earth* (12.09.2024) et. c. It is evident that these headlines are more generally related to the broader topic of China.

- "China's rise" site:wsj.com;
(www.wsj.com/search?query=china's+rise&dateRange=all&products=wsj%2Cvideo%2Caudio%2Clivecoverage%2Cbuyside&sort=relevance)

Google indicates only one headline: 'Toll of Dead and Injured Hovers Near One Million in Ukraine War' (17.09.2024). A search on the newspaper's website does not show any publications matching the query "China's rise".

- "China's rise" site:tass.com
(https://www.google.com/search?q=China's+rise+site:tass.com&client=ubuntu-s&sca_esv=827c5b7b45126b9a&channel=fs&tbs=cdr:1,cd_min:8/7/2024,cd_max:9/17/2024&ei=JEf_aajTN6GAXc8PzpuCmQ0&start=10&sa=N&sstk=Af77f_fenWmK6VYeOK36vBQiqBAwbebRBZ3aFbXAPYzkJikkE_iTjTOV3MmlpR_BKt0Whfab6MCX44Tz5_7cFtwI4WKVb9q603a8g&ved=2ahUKEwio9cvat6yUAXUhQPEDHc6NINMQ8tMDegQIMhAE&biw=1870&bih=969&dpr=1)

Google indicates 18 headlines that can be considered relevant to the search. The topic is further developed in the study.

Due to the inconsistency of the search for the phrase "China's rise", a further check was conducted using the word "China" with the following operators:

- "China" site:cnn.com;

- "China" site:wsj.com;

- "China" site:tass.com; "Китай" site:tass.com;.

The results obtained for CNN show little change, while those for The Wall Street Journal display greater diversity. In *The Wall Street Journal*, the topic of China is linked to a variety of issues, but the theme of "China's rise" is not a primary focus. Some of the headlines include:

Vatican's Meager Gains in China Spotlighted During ... (11.09.2024); *PwC China Hit With Six-Month Ban Over Evergrande Crisis* (13.09.2024); *The U.S. and Taiwan Must Change Course* (02.09.2024); *China's Forex Reserves Rose in August as U.S. Dollar ...* (07.09.2024); *What Scared Ford's CEO in China* (14.09.2024); *U.S. Officials Meet Dalai Lama in New York, Triggering ...* (22.08.2024); *China detains two activists, adding to tension with U.S* (06.09.2024) et.c.

The Google results for TASS also show considerable diversity. However, the headlines reveal an interesting tendency toward engaging public attention not only through attention-grabbing topics but also through news highlighting cooperation. This necessitated a further verification within the news agency's own platform. The examination of TASS identified over 2020 news articles, containing the term 'China' (https://tass.ru/search?search=Китай&from_date=2024-08-06T21:00:00.000Z&to_date=2024-09-17T20:59:59.000Z). From this set over 330 publications containing commentary and information on the topic of 'China's rise' are extracted. For example:

- *The Hang Seng Index of the Hong Kong Stock Exchange rose by 1.37% at the end of trading. It reached 17,660.02 points.* (17th September 2024);

- *Trump believes that China can get ahead of the US in the crypto industry The current administration of the United States is "very hostile to" this area, the former American leader said.* (17th September 2024);

- *A journalist from China said that media cooperation is gaining opportunities for joint work Wang Bin. Head of the Eurasian Bureau of the China Media Corporation, regrets that in the modern world, many media are too dependent on the politics and interests of individual countries.* (14th September 2024);

- *Zelensky called the Brazilian-Chinese peace plan destructive.* (12 September 2024);

- *China says BRICS countries should strengthen coordination in the fight against terrorism.* (12 September 2024);

- *The House of Representatives of the US Congress supported bills against China* (10 September 2024);

- *The Russian-Chinese Friendship Society considers SAMBO a part of cultural diplomacy.* (06 September 2024);

- *Expert: Biden's attack on two fronts on Russia and China doomed the United States to failure.* (18 August 2024);

- *Expert: common interests will ensure strategic stability for China and Russia. Chen Wenling, Leading Economist at CCIEE, recalled that Beijing and Moscow at the highest level announced their positions, according to which China and Russia are building transparent relations with each other* (18 August 2024);

- *India did not invite China to the summit of the Global South.* (17 August 2024);

etc.

The narratives were aimed at China's foreign activity, but also to Russia - China relationships, which reflects directly in public sphere. This category of news reports on the expansion of student collaboration and exchange, about technological cooperation, about cultural partnership initiatives (for example SAMBO a part of cultural diplomacy) etc. Due to the fact that TASS does not provide an open accessible data-structured archive, the precise temporal analysis is constrained. Nevertheless, the overall orientation of emitted narratives was evident: Russia's foreign policy increasingly directs the focus toward deepening and expanding widening Russia - Chinese partnerships.

The situation in the USA's media during the studied time-period differed substantially. Unlike most European countries, the United States does not have a single state-representative news agency — for example, an equivalent of BTA in Bulgaria, TASS in Russia, or Agence France-Presse in France, etc. For this reason, media headlines on the relevant topics were searched for on Google and in outlets such as CNN, The Wall Street Journal, and others, as well as in British media known for their active coverage of topics relating to the United States (such as Reuters or The Financial Times). There were no narratives found comparable to those identified in the RF. Even an extensive search in CNN did not yield a news headlines about China. However, within the period from 7th August to 17th September, the Wall Street Journal published a news article entitled 'China Detains Two Activists, Adding to Tension with U.S.' [21]. It is evident that the relations between USA and China are strained and this condition is inevitably imparted on the public.

It is evident that in the USA and the RF the methods for attracting public support to foreign policy are different. The observation on this topic yield that China's pursuit of a dominant role in the interstate system, has influenced the foreign policy activities of multiple countries and has engaged the publicity in these states across different periods of time.

IV. DISKUSSION

The results show that both in Russia and in the United States, China's rise is regarded as a challenge. In the spirit

of the Copenhagen School of Security, it can be said that the difference lies in the fact that in the United States this challenge is communicated as a threat, whereas in the Russian Federation it is framed as an opportunity for cooperation. This also explains the different approaches applied in the two states in order to shape public opinion regarding the challenge.

- The results of analyses argue that two diametrically positioned examples for intervention in public opinion are described. There is no doubt that the Russian activity includes both a parallel influence in multiple vectors of public interests and is looking for specific effect of accumulation. This policy leads to effective internal public support for Russian foreign relationships. As the result, the individuals in Russian publicity accept China's rise as a successful development and as an opportunity for progress.

As the result of the media policy in the USA, the interest of individuals in American publicity are organized in a pragmatic direction. That is a possible explanation of the fact that due to lack of media content people search for information across the web. It seems that in the USA China's rise is accepted as a threat for positioning in the interstate system. The coverage related to China's development either lacks in American media or are rationally directed to rational policy responses, including the development of domestic technologies, as well as a constraining of China's import among other initiatives. One example are the publications in the Wall Street Journal.

- After comparing the incidents observed during the specified period of time with representations in American media coverage, it becomes evident that publicity in the USA, independent of the Americans foreign policy interests, stays uninformed, respectively without opinion about China-Filipinos naval accident, about China's call on reassessment of the challenges before the contemporary multipolar world provided in advance of the UN General Assembly, among other events. The temporal assessment shows that they aligned with President Donald Trump's policy aimed at "bypassing" the United Nations and advancing interests in Asia [22]. From the perspective of international security, such gaps should be regarded as indicators of future actions.

- According to the contemporary concepts in the field of Security theory society constitutes a key factor for vitality of the state system. From this perspective, governments actively seek to generate and sustain public support for their activities. It is evident also that it is possible the publicity to be kept in a state of shortage of concrete information - however this manner is effective only over short temporal intervals. The results in analysis indicate that on the vector 'China's rise' information the American policy expands beyond the boundaries of this theoretical framework. An argument in this direction is the result of a Google search using the operator "China" AND "US media", which shows numerous publications outside the United States.

- One notable feature of figure 1 is the pronounced fluctuation in web-based queries on topic 'China's rise', that are emitted from the USA. This pattern suggests that individuals in the US publicity recognise China's rise as a path of foreign policy's discourse. It also indicates that with the information flows the US government may be attempting to manipulate the public support.

- The differences in media activity suggest that, in the domain of publicity, the governments of the USA and the RF employ distinctly different manners to protect their foreign policy objectives. The U.S. approach appears to involve modulated fluctuation in informational flows. In contrast, the Russian manner is founded on parallel dissemination and collaboration between media and government's initiatives. Within the Russian foreign policy discourse, China's claims about contemporary multipolar world stay in the background and are replaced with perspectives to constructive bilateral relations. This manner builds a strong public support to Russian government's initiatives.

V. CONCLUSION

1. Today, the rise of China is seen as a challenge. Some countries aim to overcome this challenge via contention (e.g. the USA), others see in this situation an opportunity for building collaboration. The situation can be defined as an example of the Thucydides Trap.

2. The management of public attitudes is an obligatory element of contention or of collaboration in foreign policy relationships through which a state overcomes the challenges in international security's environment. Irrespective of the type of attraction/repulsion of the public attention and the public support, the shaping of public opinion is necessary.

3. The approaches for management of the public opinion, which is necessary for the support of government's initiatives, vary in a wide range – from an active informational pressure to a shortage of mass information on certain topics. With this activity governments look for synergy through an accumulated effect. The connection with the Thucydides Trap indicates that the presented example is not limited to policy in Russia or the United States but is universal from the standpoint of the instruments used to shape public support.

4. Although the changes in cyberspace have been substantial, the mass media remained a significant component of activities, through which the government aimed at attracting support via public opinion. When information is insufficient and public interest is high, people seek news from foreign media outlets. This is demonstrated by the search results for "China" AND "US media".

5. The activities through which governments seek public support for their responses to a given challenge range from the cumulative shaping of public opinion – achieved through complex synergies between

governmental and media actions – to the withholding of information.

REFERENCES

- [1] Lyotard, J.-F. (2021). *Fenomenologiyata*. SONM.
- [2] A. A. Bartosh. (2021, August 12). *Gibridnaya, skrytnaya, nepredskazuemaya. Ot Gebbel'sa i Myuntsenberga k sovremennym informatsionnym bitvam*. Nezavisimoye voyennoye obozreniye. https://nvo.ng.ru/gpolit/2021-08-12/1_10_11_1153_hybrid.html
- [3] Lasswell, H. D. (1948). The Structure and Function of Communication in Society. In L. Bryson (Ed.), *The Communication of Ideas*. Harper & Row.
- [4] Smith, J. A., Flowers, P., & Larkin, M. (2009). *Interpretative Phenomenological Analysis: Theory, Method and Research*. Sage.
- [5] Allison, G. T. (2017). *Destined for war: Can America and China escape Thucydides's trap?* Houghton Mifflin Harcourt.
- [6] H. Panitsidis, O. Kasabov, and B. Popivanov, Eds., *Idei za grazhdanskoto obshtestvo. Klasicheski tekstove. Antologiya*. Sofia, Bulgaria: Universitetsko izdatelstvo "Sv. Kl. Ohridski", 2016.
- [7] V. Doncheva, "Politicheskata vlast i natsionalnata sigurnost," in *Sbornik dokladi ot Godishna universitetska nauchna konferentsiya*, vol. 1, pp. 87–97, Veliko Tarnovo, Bulgaria: Izdatelski kompleks na NVU "Vasil Levski", 2025.
- [8] D. Berchev and S. Petkov, "Irakskata kriza ot 2003 g. kato ekzogenen faktor za priemaneto na Evropeyskata strategiya za sigurnost / The Iraqi crisis of 2003 as an exogenous factor for the adoption of the European security strategy," *Pravo, politika, administratsiya (Law, Politics, Administration)*, vol. 8, no. 2, p. 24, 2021, Yugozapaden universitet "Neofit Rilski".
- [9] Palmerston, H. J. T. (1848). Remarks in the House of Commons, March 1, 1848. www.quotationspage.com/quote/41290.html
- [10] David C. Kang, Jackie S. H. Wong, Zenobia T. Chan; What Does China Want?. *International Security* 2025; 50 (1): 46–81. doi: <https://doi.org/10.1162/ISEC.a.5>
- [11] J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MA, USA: MIT Press, 1989.
- [12] S. Stoykov, S. Dimitrova, and R. Marinov, "The development of educational capacity of human resources in the field of security: Main priority of national security," IEEE, doi: 10.1109/CREBUS.2019.8840062
- [13] B. Buzan, O. Wæver, and J. de Wilde, *Security: A New Framework for Analysis*. Boulder, CO, USA; London, UK: Lynne Rienner Publishers, 1998.
- [14] P. Atanasov, *Sigurnost i komunikirane na informatsiya v publichnosta*. Plovdiv, Bulgaria: Makros, 2025.
- [15] BBC News, "China-Philippines ships collide in disputed waters," Aug. 19, 2024. [Online]. Available: <https://www.bbc.com/news/world-asia-66551256>
- [16] Reuters, "China and Vietnam agree to deepen strategic cooperation," Aug. 20, 2024. [Online]. Available: <https://www.reuters.com/world/asia-pacific/china-vietnam-agree-deepen-strategic-cooperation-2024-08-20/>
- [17] Reuters, "China and Belarus strengthen all-weather partnership," Aug. 25, 2024. [Online]. Available: <https://www.reuters.com/world/china-belarus-partnership-2024-08-25/>
- [18] Reuters, "China envoy tours Europe to push Ukraine peace plan," Aug. 28, 2024. [Online]. Available: <https://www.reuters.com/world/europe/china-envoy-europe-ukraine-peace-plan-2024-08-28/>
- [19] Financial Times, "China expands influence in Africa through investment and diplomacy," Sep. 6, 2024. [Online]. Available: <https://www.ft.com/content/china-africa-investment-2024>
- [20] Reuters, "China calls for multipolar world ahead of the UN General Assembly," Sep. 2, 2024.
- [21] Leong, C. (2024, September 6). *China detains two activists, adding to tension with U.S.* *The Wall Street Journal*. <https://www.wsj.com/world/china/china-detains-two-activists-adding-to-tension-with-washington-75942693>
- [22] UN Affairs. (2025, September 23). *US President Trump criticizes UN, NATO and climate "hoax"*. United Nations. <https://news.un.org/en/story/2025/09/1165924>

The Hybrid Warfare in Cyberspace

Plamen Atanasov

Faculty of Secure and Defence
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
atanasovp@abv.bg

Evelina Atanasova

Faculty of Security and Defence
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
evelina0823@abv.bg

Abstract— After cyberspace built its own individual image and after the opinions that this new space has potential to be a war domain, the question about opportunities for undertaking hybrid warfare in it is gaining relevance. The present study is looking for the characteristics of this type of hybrid warfare and their relations with technological sovereignty in the field of national security. This construction defines cyberspace as the object and the hybrid warfare as the subject of this study. The aim of the research is to explain the vectors of warfare in the framework of hybrid challenges that stand before states, as well as to make visible the difference in the methods of hybrid warfare. Through a multidisciplinary analysis discovered, described and arranged are different approaches, with which developed countries like China, the USA, Russia and the United Kingdom react against challenges, such as the hardware and software dependency on the cyberspace in the context of politics, economics and defence.

Keywords— cyberspace, domain, hybrid warfare, strategic approaches

I. INTRODUCTION

The research elucidates the multidimensional nature of the problem space arising from the opportunities for hybrid warfare that cyberspace provides. There is no doubt about the importance of the matter. Developments such as the US strategic interests towards Greenland in 2026 and calls for reorganization to NATO contributions reflect a crisis frame shaped, in part, by the expanding role of cyber-enabled operations. Furthermore, the EU dependence on foreign companies for the EU that own and master the management of infrastructure and software in this dimension introduces an interesting additional actuality also. It can be interfered that the attainment for technological independence (technological sovereignty) constituted an appealing yet unlikely fully realized aims. The reason lies in the existence of the factors whose nature extends beyond purely technological or digital domains. This viewpoint leads to the hypothesis that cyberspace is a comprehensive domain

for hybrid warfare. Furthermore, such warfare encompasses not only technological activities yet also extends to other spheres of our contemporary 21-st century society (e.g. industry, economy, education, everyday life et c.). Due to producing hybrid risks, cyberspace thus emerges as a source of hazards to the state system security.

The research not only aims to examine the cyberspace nature as a source of evolving hybrid threats yet also to identify the vectors through which these threats are shaped in hybrid warfare. Even the partial identification (we do not assume that their enumeration is exhaustive or that it is not subject to further development) of the vectors of hybrid warfare in cyberspace is considered a contribution to scientific research on identifying threats in cyberspace.

The research hypothesis is that hybrid warfare in cyberspace is linked to technological dependencies. This makes the achievement of technological sovereignty difficult or even impossible. The following emerge as vectors (strategic approaches) for possible counteraction to this challenge: total technological independence; control through total restriction on access; mitigation through software or hardware; complete rejection of modern digital technologies

The hypothesis shapes cyberspace as the object and hybrid warfare as the subject of the research.

For the purposes of the research, a scientific definition has adopted, grounded on the ideas of Manuel Castells about the network society, according to which cyberspace is a virtual construct constituted by infrastructure and software used to manage it, integrated into interacting communication networks and forming a coherent space in which information is processed, transformed and generated for instrumental action, e.g. in economic, in culture etc. [1,2]

It is evident that the distinction between inherently borderless nature of cyberspace and geographically bounded states sovereignty presents specific challenges for the understanding and analysis of hybrid warfare's problematic.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.131>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

The hybrid warfare, as the subject of this research, is understood as an integrated use of military and civilian instruments to achieve superiority over the prolonged time period, encompassing dominance not only in military power and governance, but also over critical infrastructure, public opinion among other societal domains. [3, 4, 5] It is evident that hybrid warfare develops in an intermediate field between the Clausewitzian understanding of war and confrontation, and the peaceful everyday life of society.

It is necessary to clarify that: Cyber warfare is understood in a broad sense and is not limited to periods of armed conflict. At the same time, it is distinguished from the narrow technical interpretation of the term; Information warfare is understood in a broad sense that goes beyond NATO's understanding of I.O.P.S.

The term "technological sovereignty" has not yet been firmly established in the academic sphere, and therefore we propose defining it as "technological independence, expressed in the capacity to produce everything necessary for a full presence in cyberspace and to utilize its capabilities."

II. MATERIALS AND METHODS

In accordance with the objective on this research, it is necessary to address the following questions: What do the hybrid wars in cyberspace encompass? Through what channels is such warfare conducted? Which states and societies are affected by such warfare? and Who is capable of conducting full-scale hybrid warfare through cyberspace?

To achieve the objective of this research, in addition to a theoretical review of existing developments, publicly available information, factual data and empirical evidence has been analyzed. During the research are used both declarative and policy documents of NATO, as well as statements of prominent politicians and relevant theoretical works addressing the issue and established as influential during the first 1/4 of the 21st century, have been used. It is assumed that such opinions, comments etc. are subsequently transformed into tendencies in everyday life. Information from internationally recognized and authoritative media sources was utilized.

The publicly available data are drawn from internationally recognized media outlets that have repeatedly demonstrated their professionalism, as well as from documents of the aforementioned organization (NATO). All sources used are listed in the References section. The media interpretations been excluded from the study.

The essence of the analysis is conceptual, and the focus is not directed toward extensive quantitative research. Such research approach is widely applied in the social sciences, including security studies, journalism, geopolitics, economic forecasting and others. For the perspective of philosophy, the security has been understanding as a stable, dynamic equilibrium as a construct that is broadly extends only in everyday human life. Therefore, the effects should be considered both in a

practical perspective (the position of policymakers) and in accordance with the social dependences (as in scientific works).

III. RESULTS AND DISCUSSION

There is no doubt that during 21st century, cyberspace constitutes one of the key domains of warfare in which military operations can be planned and executed. From this perspective, it is evident that abstract thinking enables the examination of cyberspace as an evolutionary extension of the technological developments of 20th and 19th century.

1. Results from the analysis of existing theoretical developments

It is widely recognized that in the initial stages, various researchers and early scholars (enthusiasts) examined cyberspace as a complex system composed of different interrelated subsystems, such as computers and/or computer networks.

During that time, the term 'cyberspace' was developed. In the contemporary context of national security, cyberspace is increasingly regarded as a distinct operational field, possessing a level of strategic importance comparable to the traditional war domains of land, sea, air and space. It is common practice to separate the operations in this new domain (cyberspace) according to both their aims and characteristics. In the USA the cyberspaces operations are typically categorized as follows:

- Computer network attack (CNA);
- Computer network defense (CND);
- Computer network exploitation (CNE) [6]

It is typical characteristic of CNE that it primarily involves data collection, and this activity is generally conducted covertly. [6]

Russian military doctrine distinguishes cyberspace operations into conventional and unconventional categories. Russian strategy is focused on informational superiority, which targets both the functioning of the technological systems and the control over the informational content, which can influence public opinion. Within Russian strategic discourse, discussion often includes 'unconventional' concepts such as a nanotechnological weapons, as a instruments for mass disruption, and as a capability for influencing cognitive process, although the evidence of the effective implementation of such operations is practically absent. NATO's military doctrine in cyber domain remains not fully developed. It incorporates the elements from both the concepts of informational warfare in NATO's member states and the approaches characteristics of Eastern thinking. NATO's military doctrine incorporates also the lessons learned from the practice of past conflicts.

An alternative viewpoint on cyberspace is focused on the scale and diversity of its user's base, including individuals engaged with activities such as online commerce and participation in social networks. T. Thomas underlines that the inexpensive and accessible computers facilitate this widespread use. [6]

It is obvious that relatively limited resources required to conduct large-scale operations in cyberspace, compared to a conventional military operation, make cyberwarfare increasingly preferred option for players, seeking influence within broader landscape of international competition, yet lacking capacity to afford conventional warfare. On the background of this landscape, sporadic, both successful and less successful attempts to use malicious software to sabotage systems (e.g., the viruses StuxNet—2010; BlackEnergy—2015; Petya—2017) have been leading to scandals in interstate system. In parallel with increasing interest in cyberspace sabotage activities, the past decade witnessed a significant growth in cyberattacks targeting public opinion [7]

2. Result on challenges to hybrid warfare in cyberspace

As stated in the introduction, in light of the theoretical concepts and the position presented by analysts, the research in this report is developed in accordance with the sequence of the proposed questions:

• Axes of hybrid warfare in cyberspace:

Comparative look to both M. Castell's conception of cyberspace and the NATO's position indicates that the hybrid warfare develops across the field of economics, politics, public opinion and culture, while also encompassing information warfare and psychological operations, and the deliberate disruption of critical segments of certain communication networks. According to the hypothesis in this research a key analytical focus is directed toward public opinion and culture.

• Hybrid warfare modes:

It is well established that the networks in cyberspace serve dual purposes both facilitating human connectivity and enabling the management of devices. A significant component of the latter function encompasses military applications. According to opinions that has been presented on the Munich Security Conference of February 2026, including the Aegis integrated naval system. This system integrates the management and the control across multiple operational domains, including air, sea and land environments, involving both European and American forces. [8] The views of military officials and politicians are complex. On one hand, abandoning American U.S. informational-structural systems - which effectively constitute the cyberspace component of overall architecture - would significantly diminish the operational effectiveness of this weapon complex conglomerate. On the other hand, as warned by a journal Defense Analysis editor F. Touse, acquiring such a system entails that EU states also acquire a degree of dependance on the USA. Against the backdrop of Greenland crisis, such a situation is increasingly regarded as unacceptable for the member states of the EU.

• How states overcome challenges

The contradiction between the pursuit of technological independence in cyberspace and the development of a sustainable economy is not new phenomenon and does not affect only the USA-EU interstates relationships. A similar

case emerged during the deployment of 5G networks in 2020. The infrastructure components of these networks are mainly produced in China, raising concerns regarding the potential for external manipulation or disruption, particularly in scenarios critical to NATO member states. The USA has sought to restrict the integration of Chinese infrastructure invasion and to promote the development of its own 5G system. [9]. It appears that the technology has already advanced to such an extent and has permeated so many segments of daily life that the exclusion of Chinese components renders system interoperability unfeasible. The United Kingdom places particular emphasis on protection against foreign and unwanted interference, while simultaneously adopting 5G technology largely based on solutions proposed by Chinese companies. [10] Russia also keeping pace with its strategic response. In the RF work has been underway on the project RuNet, such project aims to constrain the content, that is in contradiction to Russian inner interests. [11] Ahead the Munich Security Conference of February 2026, the French Premier minister emphasized the importance of technological sovereignty. [10]

Even the facts listed above demonstrate that the response to the challenge of overcoming foreign dominance in internet is multidimensional in nature and there is no unipolar solution.

• Society as a victim of hybrid warfare in cyberspace

The most severe manifestations of competition in cyber domain affect not only the military sphere but also society at large. This provides grounds for discussing hybrid warfare. Public opinion is confronted with a complex dilemma: military technologies inevitably evolve within cyberspace, yet this also drives technological advancement across other areas of life. Such progress requires substantial capital investments, and available data indicate that its scale is increasing as dynamically as the development of cyber technologies. According to Gartner, global IT spending amounted to 449,5 billion USD in 2013, increased significantly by 2023, and is projected to reach approximately 6,15 trillion USD by 2026. [12, 13, 14]

• Who is the winner of hybrid warfare in cyberspace

Since the Cold War has known that the affected parties are people - society and the country. People are required to purchase expensive computers and connectivity devices for data storage and protection, as without them they are unable to respond to the contemporary challenges. For example, it is no longer sufficient for one operator to coordinate the ambulances within a city region, the implication of AI is now required, as is increasingly practiced worldwide and has been shown to be more effective. However, the implication of AI requires financial resources for the acquisition of equipment and the training of personal, among other needs. This, in turn, places a burden of national economies, as such funds cannot be allocated to other priorities such as non-

computational scientific research, healthcare, urban development et c. This characteristic shift attention toward those actors that are capable of producing AI and corresponding devices. Given the evident fact that this capacity is predominantly concentrated in states as China, USA et c., it can be concluded that effective warfare – understood in the context of associated economic power – can be conducted primarily by the world’s economically developed states.

3. Discussion

The avoid presented opinions and positions indicate that there are existing multiple opportunities to warfare in cyberspace. The following categories are subjects of attack:

- the communication integrity (software and hardware) in military operations;
- public opinion and social activities through software interventions;
- the economy, i.e. economic strain caused by continuously increasing need to replace and to upgrade the digital infrastructure across multiple spheres of everyday life.

Due to this expansion is impossible that countries to withdraw from cyberspace-related activities. However, the cyberspace domain also entails a significant risk: the implementing of digital technologies may lead a state to technological dependency. It appears that the technological development in IT domain has reached such a level that is unlikely that any single state is capable of developing it independently, even if that state is among the world’s leading economies.

There is another issue present – society. This fact provides grounds for discussing hybrid warfare across cyberspace. Through cyberspace, entire economic sectors can be disrupted or eliminated, including compromising the software of a country’s power grid, or blocking the information exchange between banks.

Due to comprehensive nature of cyberspace, the risk of economic exhaustion is significantly higher, and consequently, off strain across all social sectors. Every state is exposed to such risk, regardless of its level of economic development.

TABLE 1: STRATEGIC APPROACHES AND POSSIBILITIES FOR HYBRID WARFARE AND THE ACHIEVEMENT OF TECHNOLOGICAL SOVEREIGNTY

Strategic approach	total technological independence	control through total restriction on access	mitigation through software or hardware	complete rejection of modern digital technologies
Possible examples	China, the USA, Russia and France	Russian (RuNet) China (Great Firewall)	Various states around the world	it is unfeasible in the world of the 21st century
Advantages /	Advantage : Technolog	Advantage : Indepe	Probably the most applicable	Advantage : None identified.

Strategic approach	total technological independence	control through total restriction on access	mitigation through software or hardware	complete rejection of modern digital technologies
Disadvantages	ical sovereignty; Disadvantage: Impossibility of achieving it by the third decade of the 21st century.	nance from foreign interference; Disadvantage: Contradicts the needs of the information society.	policy toward cyberspace, including warfare within it. It both allows for hybrid warfare and enables cooperation in countering threats originating from cyberspace.	Disadvantage: Contradicts the needs of the information society

This situation strongly resembles the Cold War, yet this opinion is not entirely accurate, as in our contemporary time, the poles of confrontation are more than two. As indicated above, multiple actors can be identified, including China, the USA, the United Kingdom, Russia, as well as potentially and other countries.

It may be further added that, within the cyberspace dimension, a key characteristic of hybrid warfare is its capacity to enable the systematic and multidimensional exhaustion of national economies. In response to this feature, different states pursue a variety of strategic approaches, which can be categorized as follows:

- **total technological independence:** Such attempts are observed in China, the USA, Russia and France, among others.

- **control through total restriction on access:** This option also appears to be beyond the capabilities of any individual state, regardless of its level of development. Evidence of this can be seen in the obstacles encountered by Russian RuNet initiative. Even China, which is known for the Great Firewall of China and whose technological capacity is widely acknowledged, still permits limited access to Western social platforms such as Facebook, Instagram, and Google, although this access is restricted through VPN services, roaming, corporate networks, and special permissions; [15]

- **mitigation through the adoption of foreign components combined with the development of domestic innovations aimed at risk reduction:** It should be noted however that such risk cannot be fully eliminated. A typical example can be found in use of unnamed yet remotely controlled systems (drones). It is widely recognized that they have demonstrated their operational effectiveness in the Russia – Ukraine War, during which numerous opportunities were identified for component substitution and cost reduction. At the same time, incidents

such as the coordinated denotation of explosive devices via pagers and mobile phones in Madrid in 2004 illustrate the vulnerability of communication-dependent systems. [16] or simultaneously denoted pagers used by Hezbollah activists in Lebanon in 2024. [17] Hybrid, asymmetric, or however this operation may be named, its demonstrates that in information technologies it is hardly feasible to establish control over hardware and software and supply chains that is acceptable to all states;

• **mitigation through software and control, with emphasis placed on the programming and hardware within cyberspace.** Consistent with the understanding that software constitutes a key element of hybrid warfare in cyberspace, statements by British Computer Society highlight this perspective. In the British view, programming is understood not only as a technical discipline but also as an ethical practice and a component of the hybrid security environment. In line with the European tradition, it is further argued that programming is no longer merely an engineering activity, yet one with significant socio-political implications. [18] In this context, similar perspectives also reflected within NATO. According to this view, it is increasingly difficult to draw a clear distinction between civilian and military software. As a result, private IT companies face the risk of becoming unintended participants in cyber warfare and related hybrid conflict dynamics; [19, 20]

• **theoretically, it is possible a country to address this challenge through a complete rejection of modern digital technologies**, i.e., computers and network systems. However, no such case is known in practice, and such an approach is highly unlikely to be realized in the context of the 21st century challenges.

Table 1 summarizes the results of the hypothesis verification in the present report.

IV. CONCLUSIONS

In the contemporary context, a clear distinction between civilian and military applications of software and hardware has become increasingly difficult to maintain. Likewise, the realization of comprehensive control over communication in cyberspace appears increasingly unattainable.

The achievement of absolute technological sovereignty appears to be unattainable, at least in our decade.

In this context, the hybrid warfare is increasingly extending into cyberspace. This expanded form of hybrid warfare is grounded in the competition between the pursuit of technological sovereignty, the contested feasibility of achieving such technological sovereignty and the risk of economic exhaustion.

Placed in such an international security environment, the state's efforts to respond to the challenge can be divided into four groups:

- achieving total technological sovereignty. Such an objective is difficult, if not unattainable, to achieve;

- establishing comprehensive control over communication in cyberspace, an outcome whose feasibility remains doubtful;

- accepting imported components while simultaneously developing domestically produced technologies, with particular emphasis placed on software development.

- total isolation from cyberspace, a course of action that is unlikely to be feasible.

There is no doubt that cyberspace creates conditions for complex, multidirectional, and fully hybrid warfare. The balance between risk acceptance, objective assessment of one's own capabilities, and the avoidance of the threat of economic exhaustion is a determining factor for success in this form of warfare.

REFERENCES

- [1] M. Castells, *The Rise of the Network Society*. Oxford, U.K.: Blackwell Publishers, 1996.
- [2] M. Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford, U.K.: Oxford University Press, 2001.
- [3] F. G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA, USA: Potomac Institute for Policy Studies, 2007.
- [4] North Atlantic Treaty Organization (NATO), "Wales Summit Declaration," Brussels, Belgium, 2014.
- [5] North Atlantic Treaty Organization (NATO), "Warsaw Summit Communiqué," Brussels, Belgium, 2016.
- [6] T. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*. Fort Leavenworth, KS, USA: Foreign Military Studies Office, 2011.
- [7] P. Atanasov, *Sigurnost i komunikirane na informatsiya v publichnostta*. Plovdiv, Bulgaria: Makros, 2025.
- [8] H. Foy, B. Moens, L. Petel, C. Clover, and S. Pfifer, "Europe's 'tech sovereignty' ambitions carry security risks, military warns," *Financial Times*, Feb. 24, 2026. [Online]. Available: <https://www.ft.com/content/0f7f7aa7-af4e-4ea6-82da-5f8c719982fe>. Accessed: Apr. 27, 2026.
- [9] *Financial Times*, "China expands influence in Africa through investment and diplomacy," Sep. 6, 2024. [Online]. Available: <https://www.ft.com/content/china-africa-investment-2024>. Accessed: Apr. 27, 2026.
- [10] B. Belyaev, "5G in the Old World: Why U.S. allies choose Huawei," *TASS*, Jan. 30, 2020. [Online]. Available: <https://tass.ru/mezhdunarodnaya-panorama/7632815>. Accessed: Apr. 27, 2026.
- [11] D. Zubarev, "Runet as a political space: The transformation of Russian online media," *Russian Politics*, vol. 2, no. 1, pp. 74–95, 2017.
- [12] Gartner, Inc., "Global Government IT Spending," 2013. <https://businesstech.co.za/news/it-services/40420/global-govt-it-spend-seen-flat-in-2013/#:~:text=Global%20IT%20spending%20by%20government%20organisations%20is%20projected,organisations%20on%20hardware%2C%20software%2C%20IT%20services%20and%20telecommunications>.
- [13] Gartner, Inc., "Worldwide Government IT Spending Forecast and Trends," 2023. <https://economymiddleeast.com/news/governments-worldwide-to-spend-589-8-bn-on-it/#:~:text=Worldwide%20government%20IT%20spending%20is%20forecast%20to%20total,new%20report%20released%20by%20management%20consulting%20company%20Gartner>.
- [14] Gartner, Inc., "Worldwide IT Spending Forecast 2026," 2026. <https://marketanalysis.com/gartner-global-it-spending-to-hit-6-31-trillion-in-2026-driven-by-ai-infrastructure/#:~:text=Worldwide%20IT%20spending%20is%20projected%20to%20reach%20%246.31,AI%20infrastructure%2C%20high-performance%20compute%2C%20and%20advanced%20memory%20technologies>.
- [15] M. E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton, NJ, USA: Princeton University Press, 2018.

- [16] Spanish Ministry of the Interior, “Report on the March 11, 2004 Terrorist Attacks in Madrid,” 2005.
- [17] Reuters, “Hundreds injured in Lebanon after Hezbollah pagers explode in coordinated attack,” Sep. 17, 2024. [Online]. Available: <https://www.reuters.com/>. Accessed: Apr. 27, 2026.
- [18] British Computer Society, “BCS Code of Conduct and Ethical Guidelines,” 2023. [Online]. Available: <https://www.bcs.org>. Accessed: Apr. 27, 2026.

- [19] North Atlantic Treaty Organization (NATO), *NATO Strategy on Countering Hybrid Threats*, 2022. [Online]. Available: <https://www.nato.int>. Accessed: Apr. 27, 2026.
- [20] European Centre of Excellence for Countering Hybrid Threats, *Hybrid Threats and Resilience in Cyberspace*, 2021. [Online]. Available: <https://www.hybridcoe.fi>. Accessed: Apr. 27, 2026.

Challenges and Achievements in the Education in the Gender Perspectives in Security and Defense's Common Module

Nevena Atanasova – Krasteva

National and Regional Security Department

Vasil Levski National Military University Veliko Tarnovo, Bulgaria, nevena_atanasova@abv.bg

Abstract: *Military academies and universities in Europe are looking for ways to harmonize military education and training of future officers to increase interoperability of the EU member states' armies. The rich history of the "European Initiative of Exchange of Young Officers, inspired by Erasmus+" is a proof of successful initiatives, as it offers attractive international training, with one of the modules offering training on understanding and implementing gender equality policies in the military environment. This report includes an analysis of the learning content and the results of the feedback from the trainees in the last two editions of the Common Module, organized by the military academies of Italy and Greece.*

Keywords: *Gender perspectives, military education, CSDP, Military Erasmus.*

I. INTRODUCTION

The armed forces of NATO and EU member states have increasing commitments due to current conflicts in different parts of the world, which necessitates the application of flexible models in the training of female and male military personnel and the development of capabilities such as: critical thinking and analysis, developed skills for working in a gender-mixed environment, mastery of strategic communication processes and many others. The above and other capabilities and competencies require an interdisciplinary approach in their preparation and development, as well as coordination at various levels to internationally achieve compatibility and applicability.

The education of university graduates in the professional field of Security and Defense is a national commitment that is oriented and increasingly changing according to modern requirements for transparency and compatibility of development of the military systems of the armies of the EU member states. The Sectoral Qualification Framework for the Military Officer Profession (SQF-MILOF), completed in 2020, as part of the Common European Qualification Framework, offers the main guidelines in the content of the knowledge, skills and competencies necessary for the qualification of

military experts who are to provide adequate solutions and shared responsibilities in managing threats and conflicts in the 21st century. The framework, developed with the support of the EU Military Committee, provides practical guidance and offers a platform for following standards in military training in order to ensure interoperability and harmonization of the preparation of future military and civilian leaders in the sphere of security and defense. [11]

At the same time, the Sectoral Qualification Framework for the Military Officer profession encourages the exchange of training opportunities offered by different EU Member States and their military educational institutions. Comparative analyses of educational programmes with a view to their cooperation and upgrading allow the creation of a uniform content of academic training courses that are also recognized in other countries. This ensures the exchange of knowledge and skills in the professional field and creates conditions for the development of shared values and common culture in Security and Defence. [2]

In this regard, one of the challenges facing military leaders is their preparation for working in a gender-mixed environment, along with the need to develop skills to implement a gender perspective in peacetime and during missions and operations. Despite the fact that women actively entered the military environment more than 30 years ago and serve in all positions in the Armed Forces, gender stereotypes still exist. The prejudices of military personnel, together with the ignorance of the international framework on women, peace and security, often cause discriminatory attitudes, restrictions on career development and deterioration of the socio-psychological climate in the military teams. In addition, lessons learnt from modern missions and operations reveal the need to train military personnel in international humanitarian law, increase sensitivity to the traditions and customs of the local population, along with respect for their culture and ensure the protection of the most vulnerable groups - women, children and the elderly.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.155>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

For this reason, training in the essence of the gender equality policies, the specifics of applying these policies in the professional field of Security and Defense, is a tool for reliable training of military personnel. Education in the effective inclusion of gender perspectives both in daily activities and in planning missions and operations would lead to the creation of a sustainable environment for the development of the potential of each team member, stimulating cohesion and support, as well as the successful implementation of various military tasks.

II. MATERIALS AND METHODS

It is worth noting the mutual relationship between the sectoral application of the European Qualifications Framework in officer training and the EU Common Security and Defence Policy (CSDP).

As the EU High Representative for Foreign Affairs and Security Policy states in the foreword to the 4th edition of the CSDP Handbook, "The Common Security and Defence Policy (CSDP) is the global 'business card' of our Union (the European Union – author's note) when it comes to crisis management. A well-functioning CSDP with its missions and operations is crucial for the implementation of our priorities under the Global Strategy, namely security and defence, building the resilience of states and societies, adopting an integrated approach to conflicts and crises, strengthening the joint regional order and establishing a rules-based system of global governance." (Handbook on CSDP, 2021)

In short, the EU CSDP plays a key role in the Union's foreign policy, with its activities and tasks aiming at the development of its own defence capabilities, international crises and conflicts response capabilities, which would contribute to strengthening peace and security. To achieve the aforementioned objectives, the CSDP relies on instruments such as: civilian and military missions and operations; deepening defence cooperation between Member States; financing scientific developments through the European Defence Fund; functioning of an EU Military Staff for coordination at a strategic level. [5] It can be summarized that the EU CSDP should be seen as a complex, combined model of coordination between the individual governments of the member states and supranational integration.

The analysis continues in the direction of searching for a connection between the EU CSDP and the Sectoral Qualification Framework for the military officer profession, where one can find structural and functional dependencies. If the European Qualification Framework provides the educational level and formation of competencies for future military leaders, then the CSDP offers the political support and operational implementation of the competencies built.

Conceptually, this relationship can be viewed in the sequence: educational base - capability building - conducting missions and operations. Since the EQF is structured in eight reference levels, oriented towards learning outcomes, these same levels cover all types of general qualifications - from basic to advanced. [10] In

the military environment, the comparability of qualifications is specified through the Sectoral Qualifications Framework, which offers a definition of the officer profile in terms of knowledge, skills and competences, which significantly facilitates educational exchange and the recognition of completed training by higher military educational institutions in EU countries. Thus the effect and the desired end state of professional compatibility of military training are achieved.

On the other hand, the CSDP has the political instruments for crisis management of various kinds, the deployment of military and civilian missions, using national military assets. The need to achieve a high degree of interoperability is necessary to realize the collective military capability of the EU and to promote a strategic security culture.

Historically, since its creation, the CSDP has evolved, transformed, expanded, gradually incorporating new initiatives and instruments. As a result of the growing influence of UN Security Council Resolution 1325 on Women, Peace and Security and subsequent resolutions forming the Women, Peace and Security Agenda, gender equality has been incorporated as an essential component of the contemporary notion of security.

"The EU gender mainstreaming policy in crisis management is based on mainstreaming, i.e. the systematic integration of gender equality into all areas of CSDP, from the planning and implementation of missions and operations to reporting, evaluation, training and lessons learned. The ultimate goal of gender mainstreaming policy in CSDP is gender equality, one of the fundamental values of the European Union, underlying in the Treaty on European Union. " (Handbook on CSDP, 2021, p. 139)

In CSDP, gender equality is implemented by applying a gender perspective in all stages of the policy - from planning through implementation to evaluation of missions and operations, which we call gender mainstreaming. The practical implementation or specific operationalization of gender policies within CSDP missions is carried out by appointing gender advisers and experts (gender advisers or gender focal points), conducting gender analyses to assess the impact of decisions on different social groups or the local population, as well as gradually integrating the gender perspective into the operational planning process of operations. [4]

In a number of foundation-laying documents, some of which mentioned above as sources that describe the substantive aspect of gender mainstreaming policies, training is indicated as a key tool. Gender mainstreaming training is part of the preliminary preparation for EU missions and operations, but also a supporting process during and after the participation itself, as capacity building is necessary for the effective implementation of these policies. [3]

The European Security and Defence College (ESDC) is a leading institution in the field of gender equality

policy training for the EU. The autonomous EU structure is committed to promoting peace and stability by offering a range of educational initiatives aimed at civilian, police, military and diplomatic personnel to prepare them for dealing with current security threats. [9] In this regard, various trainings are offered related to the preparation of equality advisors, integration of gender perspectives in CSDP missions and operations, implementation of the main pillars of the Women, Peace and Security Agenda in EU policies, as well as training on the recognition and prevention of sexual violence, assault and gender-based violence during conflicts.

Undoubtedly, one of the most successful structures of the ESDC is the "European Initiative for the Exchange of Young Officers, inspired by Erasmus+", also called Military Erasmus for short. The initiative offers a wide range of activities - international semesters, common modules, workshops and meetings, strategic partnership projects, etc., with the aim of achieving harmonization of military training in Europe and increasing the interoperability of the armies of the EU member states. [8] By promoting educational mobility and exchange of students and academic staff from different military academies and universities, the high level of preparation and training of future military leaders is stimulated, as well as the formation of an adequate attitude and understanding of the contemporary challenges facing international security. For more than 15 years, the Initiative has achieved real results through the voluntary participation of European military academies, which are highly appreciated by national and European institutions, as Military Erasmus is the main common tool for the development of mobility with a focus on higher military education. [6]

The Lines of Development are the main directions in the Initiative, which provide educational offers for the different services of Armed Forces and for all professional areas in the Security and Defense sector. In relation to the topic of this report, it should be noted that Line of Development 10 – Gender mainstreaming in the Armed Forces (Line of Development 10 – Gender mainstreaming, <https://www.emilyo.eu/lod-10-gender-mainstreaming>) has been one of the most successfully and rapidly developing ones in the last 5 years. The organizing of annual seminars on the implementation of gender equality policies in the military environment, the implementation of a strategic partnership project with the participation of military academies from Bulgaria, Italy, Portugal and Romania, the organization of training in the Common Module "Gender Perspectives in Security and Defense" in 6 editions are proofs of the interest in including this training in the knowledge and skills of future security experts and military leaders.

Each Common module "Gender perspective in Security and Defence" was developed with the assumption that the theoretical sessions, practical sessions such as case studies and role-playing games included in the training program would contribute to raising the awareness of the future military leaders about gender

equality policies and changing their attitudes about the need to include a gender perspective and analysis in the planning of military operations.

III. RESULTS AND DISCUSSION

This report is a continuation of a previous publication on the topic, related to the results of training in international environment in "Gender Perspectives in Security and Defense" Common Module. The module has been developed by a team of experts from European military academies and has undergone a strict procedure for compliance with the requirements of the Sectoral Qualification Framework for the Officer Profession. The high ratings of the trainees who participated in the first editions of the Common Module, as well as the positive feedback and recommendations from the academic staff participants - lecturers and observers, allowed for the improvement of the content of the offered training on gender equality issues. [1]

The educational content of the Common Module, in which cadets and students from European military academies and universities receive in an international learning environment, is related to competences about the following: [7]

- key concepts of gender, gender equality, gender mainstreaming, gender stereotypes;
- UN Security Council Resolution 1325 and the Women, Peace and Security Agenda;
- international framework of gender equality policies - EU Gender Strategy and NATO Action Plan, Governance and Mainstreaming;
- content of gender education in military training environments, good practices and lessons learned related to gender mainstreaming in EU military academies;
- conflict-related sexual and gender-based violence as tactics of modern warfare;
- content of gender analysis and gender diversity analysis in operations and missions;
- inclusion of equality management to achieve operational effectiveness;
- liaison and coordination with external actors in implementing equality policies and training of advisors and experts.

An integral part of the training in each module is the linking of theoretical knowledge with practical discussions, role-play, case studies, syndicate work and presentation of trainees' solutions. The educational framework of the module allows for its tailoring and updating in accordance with the feedback received from the participants, as well as according to the capabilities of the military academy/university - host of the General Module and the expertise of the international team of lecturers providing the training.

In this regard, the survey method, which was developed by the military experts at the European

Security and Defence College, is used as a research method to obtain feedback from training participants. The survey is conducted at the end of each module by providing it online to all trainees, who are invited to answer the questions anonymously. For each Common module, a specific questionnaire is offered, related to the training topics and practical activities performed by the participants.

The survey included 24 questions, which include: demographic characteristics of the participants - gender, country, type of Armed Force; assessment of training achievements; assessment of the content and teaching method of each session of the module; self-assessment of English language skills for an active participation in the working sessions; level of understanding of the English language of the lecturers; assessment of the level of administration of the module and the technical conditions of the host academy; correspondence of the knowledge provided to its importance for the professional life of each trainee; assessment of the overall conduct of the module; level of recommendation to the colleagues of the participants to participate in similar training; assessment of the full engagement of the trainees' attention; assessment of the level of applicability of the knowledge obtained and assessment of the extent to which the content of the training was in line with the expectations of the participants.

The scales used for answering the questions, according to their specificity, are of two types. In one case, specific answers are indicated with variations as follows: not achieved, very limited achievement, only partially achieved, largely achieved, fully achieved, exceeded expectations. In the other case, the rating scale is from 1 to 6, where one denoting the total disagreement with the argument and six means the total agreement. The last question of the survey is an open-ended question, in which participants give their assessment of the overall organization of the Common module in free text and make comments and recommendations for improving its future conducting.

Quantitative methods were applied to process the data obtained, revealing general and specific trends regarding the content of each learning interaction or the level of overall satisfaction with the training. It is assumed that scores between 4 - 4.50 and 6 are evidence of the high level of the included training sessions and of successful learning outcomes as a desired end state.

In the 6 trainings conducted so far in the Common module, organized by various military academies in Europe, an average of 25-40 cadets and students from Europe, USA, Canada and Asia have participated. If we assume that the participants - representatives of various military academies are a representative sample of their Armed Forces, then the inclusion of all trainees in obtaining feedback at the end of the training in the Common module is a general population. This allows for observing trends, drawing careful conclusions and proposing an update of the educational content.

The research question in this report is related to the hypothesis that updating the learning content of the module in each edition as a result of the feedback received from the participants in the previous edition leads to an improvement in the perception of the content of the included topics through the proposed new questions and discussions, a variety of practical pedagogical methods and enhances the involvement of the trainees in the educational impact. In turn, this would lead to higher satisfaction of the participants in the training and to motivation for the teaching team to constantly expand and change the content of the module in order to more fully achieve the learning outcomes.

The Italian Army School, part of the University of Turin, Italy, hosted the 5th edition of the Common Module "Gender Perspectives in Security and Defence" in October 2025. As shown in Fig. 1, the module was attended by 47 civilian students and cadets from military academies and civilian universities from Belgium, Bulgaria, Greece, Italy, Poland and Romania, of whom 20 were women (43%) and 27 were men (57%). The cadets represented all branches of the Armed Forces (Army, Air Force, Navy), and 12 of the participants were students in the professional field of "Security and Defence" from Italy and Romania.

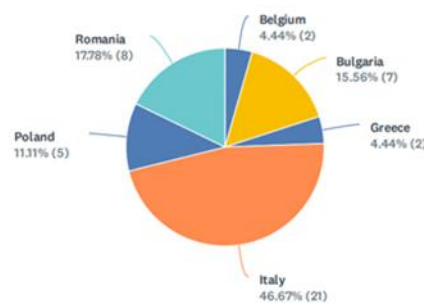


Fig. 1. Participants by country in the Common Module "Gender Perspectives in Security and Defense", Turin, 2025

The international team of lecturers included 8 lecturers from military academies and universities in Bulgaria, Italy, Portugal and Poland. The lecturers and instructors had academic as well as mission and operational experience, and with their competences in the field of implementing gender equality policies in military training, contributed to the quality of the theoretical and practical sessions. In addition to the basic and mandatory lectures for the module on understanding gender in a physical and social context, resolution 1325 "On Women, Peace and Security", international documents and policies for implementing and managing gender equality as a factor of security. The module program included discussions and case studies on the following topics:

- gender mainstreaming in the CSDP architecture – tools and implementation process;

- gender perspective, messages and reflection in communication in military environments;

- sexual violence in conflict and post-conflict environments.

The trainees were also introduced to the results of the research from the Strategic Partnership Project “Gender Research in Military Environments”, as well as to the Italian version of the “National Action Plan under UN Security Council Resolution 1325”.

Each Common Module is subject to control and analysis by the European Security and Defence College regarding the results of the training. In this regard, all trainees are required to fill out an online questionnaire at the end of the module and give an assessment of all aspects of the organization and conduct of the module, such as: comprehensibility and accessibility of the content of the lectures and practical sessions, improvement of the level of English proficiency, usefulness of the training and further application, organizational and technical support from the host academy, recommendations for improving the next iterations of the module, etc.

This paper presents part of the results obtained, which feedback from the trainees is necessary for the overall assessment of all components in the organization and the conduct of the international training.

Q4 Evaluate the achievement based on learning outcomes as defined in the respective course Curriculum. The participant at the end of the course should be able to:

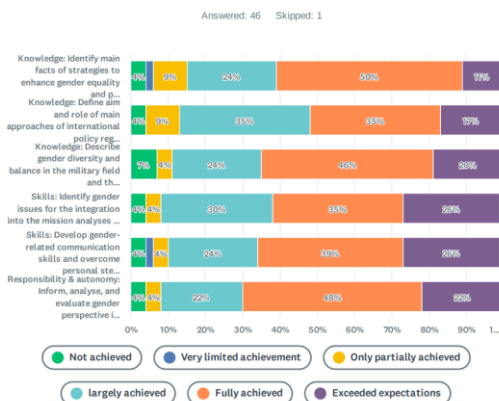


Fig. 2. Response of participants in the General Module regarding the assessment of learning outcomes

Fig. 2 presents the participants' summarized assessments of their achievements based on the learning outcomes as set out in the relevant course curriculum.

Regarding the knowledge of identifying the main facts of strategies for improving gender and equality, 50% of the participants stated that the training had fully achieved its objectives, and for 11% of the cadets and students, participation in the module had exceeded their expectations.

Regarding the question related to the ability to define the purpose and role of the main approaches of international policy for implementing equality, 35% of the participants believe the training results had been fully achieved, another 35% say they are greatly achieved and 17% say they have exceeded their expectations.

The remaining questions concerning the knowledge gained about gender diversity and balance in the military field; the identification of gender issues and their analysis when integrated into missions, the development of gender-related communication skills and overcoming stereotypes regarding gender and their social roles, etc., have received similar answers as the ones mentioned above. The high evaluation scores received, predominantly in the values from "achieved to a large extent" to "exceeded my expectations", are evidence of the very good preparation offered to the trainees. It is not surprising that the participants gave a very good rating for the overall implementation of the module - 4.9 on a six-point scale, and the average value of the trainees' assessment that they understood how to apply the information learned during the module in the future - 5.14, is another indicator of the desired results achieved.

Young people, representatives of Generation Z, are extremely sensitive to the topics discussed in the module and readily share their recommendations for its improvement, related to: improving the preliminary online preparation for the module; more effective time allocation; more practical activities in working groups and other issues of a domestic or organizational nature.

The general feedback assessments by the trainees participating in the Common Module "Gender Perspectives in Security and Defense", held at the Italian Military School, can be grouped around the following statements:

- "Very interesting lectures, which I consider extremely important from the point of view of future participation in CSDP missions and operational activity.";
- "I did not have high expectations at the beginning, but I am happy that I took this course because it made me explore important topics that I had never analyzed in such depth before and which I consider to be of paramount importance.";
- "It was a great experience with a lot of useful things to learn."

The next edition of the Common Module “Gender Perspectives in Security and Defense” as part of the Military Erasmus educational initiatives was held in February 2026, hosted by the Hellenic Air Force Academy and the Hellenic Military Nursing Academy in Athens, Greece. The participants were 32 cadets and 2 students from Greece, Cyprus, Portugal and Romania, 21 of whom were women and 13 were men. The trainees represented military academies of the Land Forces, the Air Force, the Gendarmerie, the Academy of the Ministry of Interior and civilian universities. The lecturers were 8 professors from Bulgaria, Greece and Portugal, as well as equality experts from the General Staff of the Hellenic Army.

The organizers from the Hellenic Military Academies also proposed new lecture topics to be included in the instructional content, related to understanding the gender perspective and the application of equality policies in

peacetime and conflict management processes, in accordance with the CSDP recommendations. The new topics offered knowledge and practical role-plays and case studies in the field of:

- the essence of collective security and peacekeeping mandates: legal, operational dimensions and gender perspective;
- CSDP missions and operations - gender language in mission mandates;
- gender diversity and sexual harassment;
- artificial intelligence - is it gender neutral? Gender stereotypes portrayed through artificial intelligence;
- strategic communication, psychological operations and gender narratives;
- gender-sensitive decision-making in peace and security support operations.

The very good preparation of the lecturers as well as the correct choices of pedagogical approaches received an extremely high rating from the trainees at the end of the module when evaluating all aspects of the training provided, as it can be seen in Fig. 3.

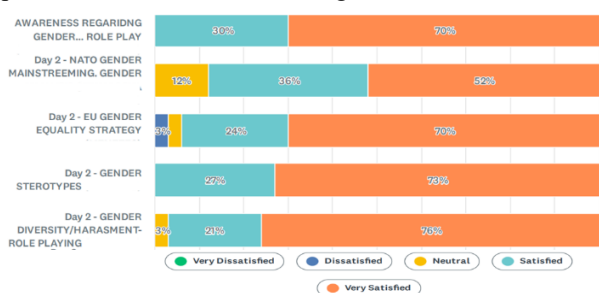


Fig.3. Responses from the Common Module participants in Greece regarding the evaluation of the content of the different topics and the pedagogical method for teaching them

A careful analysis of the feedback received gives a reason for satisfaction with the results achieved, as an average of 50 to 70% of the trainees share their complete satisfaction with the received training and the way the specific information has been presented. The remaining 25 to 35% of the trainees are also satisfied with the knowledge gained, which is a good certificate for the inclusion of new interesting and hot topics, tailored to the management of equality in current realities and technological challenges.

The overall assessment of the results obtained from the training conducted at the Hellenic Military Academy of Nursing, according to the feedback received, is very high, which is due to the effective pedagogical approaches, as well as the attractiveness of the mandatory and of the new topics included, taking into account the specifics of the General Module. (Fig. 4)

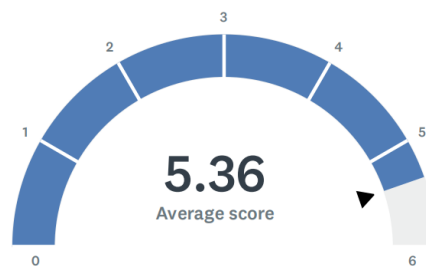


Fig. 4. Responses of participants regarding the overall quality assessment of the Common Module in Greece

It is worth noting here that the overall evaluation of the module in Greece is higher than the feedback received on the same question from the participants in the Common Module held in Italy, which is 4.86. Despite the very good evaluations of the various elements of the module implementation by the Italian Army School, as indicated in the previous analyses in the report, taking into account the participants' comments to improve the module content has led to an increase in the positive evaluations. This evidence confirms the hypothesis set out in the research question that the analysis of the feedback from participants in any educational initiative is a reliable tool for the content of the education and training, and its relevance and applicability.

The trainees who successfully completed the gender related training and received sufficient information about the applicability of their knowledge in future professional practice say that they would definitely recommend this module to their colleagues – 97%. In addition to the positive feedback from the trainees, the participants are always encouraged to share elements that they did not like or other ideas to optimize the learning interaction. It is striking that the recommendations regarding the availability of more practical scenarios and conducting seminars/games are extremely similar to the recommendations of the participants in the General Module in Italy. This is not surprising, given the similar characteristics and values of the generation that mainly represents student youth in Europe, a generation which seeks dynamics, diversity and needs to be always convinced of the usefulness of the knowledge received, aiming to turn this knowledge into skills and develop into competencies.

The overall impression from the responses to the 24 questions in the survey, related to the evaluation of all aspects of the proposed training, reveals the high level of satisfaction of the participants from different countries. More than 90% of the shared opinions of the trainees are in a positive light regarding the usefulness of the knowledge gained, as well as the good assessment of the need for such training in a military environment. (Fig. 5)

Personally I was more than satisfied from this Common Module, I look forward to the next one.	2/20/2026
It was a great and unique expert	2/20/2026
I would participate again	2/20/2026
Thank you for the amazing experience and the insight we gained as long as the new meets with expertised officers and students from other academies	2/20/2026
During this course, I gained a deeper understanding of how gender perspectives directly impact operational effectiveness. I learned that ignoring gender can create intelligence gaps and increase security risks. Integrating gender perspectives is not about politics or ideology — it is about making missions more successful, more trusted, and better informed. The course also strengthened my sense of responsibility as a future officer. Even at a junior level, I can help identify blind spots and promote more inclusive and effective operations.	2/20/2026
Very good	2/20/2026
module was very interesting, the group was top and the teachers very interactive	2/20/2026

Fig. 5. The feedback of the course's overall organization of the Common Module in Athens, Greece

Although some of the trainees demonstrated some distrust at the beginning of the module, even discomfort from discussing topics related to equality and gender stereotypes, their open behavior at the end of the training and the free interpretation of specific policies are evidence of successful interactions with the trainers. In addition, the positive feedback together with the recommendations of young people for improving the next editions of the module engage the creators of training content with a constant analysis of changes in policies for implementing equality in the military environment, the study of good practices, taking into account generational differences and other factors influencing the achievement of the desired knowledge, skills and competencies in the field of gender mainstreaming.

IV. CONCLUSIONS

In conclusion, it can be summarized that the feedback received from cadets and students from all over Europe who successfully completed their training in the Common Module "Gender Perspectives in Security and Defense", offered by the European Initiative, showed the relevance of gender education. The very good grades are an indicator of the high degree of achievement of the training results in implementing equality policies in the military environment, which would contribute to building a qualitative competence profile of future officers.

The feedback analyses have a direct link to the answer to the question of how relevant is education in gender equality policies in the field of Security and Defence to the challenge of overcoming gender stereotypes and integrating a gender perspective into military activities in peacetime and during conflicts. The data show that education, combined with adequate practical and applied methods, is an important resource for promoting

understanding of gender equality policies and influences the increase of the operational capacity of the Armed Forces.

The complex interdisciplinary relationship between the various thematic areas that relate to and influence gender perceptions needs to be specified and directed towards proper incorporation into the security system. This leads to the conclusion that gender equality is not an incidental element in CSDP, but should be perceived as a structurally integrated component of this policy. Strategic documents related to the gender equality policies are operationalized through the relevant mechanisms, offering diverse training and preparation for the officers for an effective management of military formations, taking into account the needs of both sexes and developing their talents.

REFERENCES

- [1] Atanasova – Krasteva, N., Gender perspectives training in the international military educational environment, Union of Scientists in Bulgaria, Science Days, Veliko Tarnovo, 2024, pp.158–168
- [2] Dimitrov, Nedko, Overview of the Qualification frameworks, Bulgarian case, Research, Analysis, Foresees, Voenen Zhurnal, 4/2023, pp.370–382
- [3] European External Action Service (EEAS). (2019). EU Action Plan on Women, Peace and Security (2019–2024).
- [4] European External Action Service (EEAS). (n.d.). Gender in CSDP missions and operations.
- [5] Handbook on CSDP, Volume I 4th edition, edited by Jochen Rehr, Federal Ministry of Defence of the Republic of Austria, 2021, pp.18–209
- [6] PAILE-CALVO, Sylvain, From European mobility to military interoperability, Luxembourg: Publications Office of the European Union, 2016, pp.9–68
- [7] Common Module Gender Perspectives in Security and Defence, https://www.emilyo.eu/sites/default/files/VC_LOD_documents/LoD_08_Common_modules, [Accessed April 15 2026].
- [8] European initiative for the exchange of young officers inspired by Erasmus, <https://www.emilyo.eu/> [Accessed April 13, 2026]
- [9] European Security and Defence College, <https://www.esdc.europa.eu/about-us> [Accessed April 13, 2026]
- [10] European Union, 2009. European Qualification Framework [online]. Available from: <https://europa.eu/europass/en/european-qualifications-framework-eqf> [Accessed April 12, 2026]
- [11] Sectoral Qualification Framework for the Military Officer Profession (SQF-MILOF), European Security and Defence College, https://www.esdc.europa.eu/configurations/sqf-milof_en [Accessed April 9, 2026]

The Crisis Around Greenland and the Test for NATO and the European Union: Legal Limits of Territorial Claims and Tools Against Coercion

Daniel Berchev

Security and Defense Faculty
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
dberchev@nvu.bg

Monika Panayotova

International Economics and Politics Faculty
University of National and World Economy
Sofia, Bulgaria
monika.panayotova@unwe.bg

Abstract – The study analyzes the geopolitical crisis surrounding Greenland as a fundamental test of the sustainability of the international legal order and the institutional capacity of NATO and the European Union (EU). The focus is on the conceptual clash between the outdated model of “territory purchase” and the modern liberal legalism affirming the right to self-determination of the Greenlandic people. The methodology includes a legal and normative analysis of the 2009 Act on Greenland Self-Government, a comparative study of the evolution of the Monroe Doctrine, and an analysis of cases of geoeconomic coercion in the Arctic. The results of the study identify critical risks arising from the increased Russian-Chinese strategic cooperation and the vulnerability of critical infrastructure to foreign investment. The main conclusions reject the treatment of territory as a commodity and emphasize that sovereignty is inextricably linked to the will of the population in Nuuk. The article recommends, on the one hand, institutionalizing NATO's role by strengthening its European pillar and eliminating the “alliance dilemma” by conducting a specialized Arctic mission, and on the other hand, activating the EU's defense mechanisms against economic coercion and strictly adhering to the democratic procedures for changing the status, as set out in the 2009 Act. The study establishes Greenland as an active security entity, whose defense is a litmus test for the ability of Western allies to uphold the principle of sovereign equality and to implement an innovative approach in a “zero to one” perspective.

Keywords – Arctic, European Union, International Law, NATO

I. INTRODUCTION

The relevance of the study is determined by the growing tension in the Arctic, which transforms the region from a zone of low tension into a field of geostrategic competition, questioning solidarity in NATO and the

European Union (EU). In this context, the revitalization of American interest in Greenland, often interpreted as a modern update of the Monroe Doctrine, puts transatlantic solidarity and the international legal order to the test. The case of Greenland, which occupies a central place as the “Arctic gateway” of North America, is not just a bilateral dispute between Washington and Copenhagen. It is a fundamental test of the international legal order and the ability of Western institutions to protect the sovereign equality of their members against instruments of geopolitical coercion. In view of the fact that Greenland is becoming a “transshipment point” for strategic interests, it ceases to be a simple geographical territory and becomes a test of the sustainability of the international order.

Therefore, in this publication, the object of study is the contemporary geopolitical and international legal status of Greenland in the context of the transformation of the Arctic into an operational theater of global strategic rivalry. This includes the dynamic relations in the USA-Denmark-Greenland triangle and the role of the island as a critical element in the design of security in the North Atlantic. The subject of the study focuses on the legal boundaries of territorial claims to Greenland, which outline the boundaries of permissible territorial and economic claims in the 21st century, analyzed through the clash between state-centric realism and liberal legalism. Special emphasis is placed on the right to self-determination, enshrined in the 2009 Act on Greenland Self-Government, and the specific political and legal instruments of NATO and the EU to counteract geopolitical and economic coercion. In this sense, the aim of the article is to prove that in the modern era of liberal legalism, territorial integrity is inextricably linked to the right to self-determination, which makes the classic models of “buying and selling” of territories legally null and void. The article also seeks to outline the role of NATO and the EU as guarantors of preserving the status

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.87>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

quo in the Arctic by combining military modernization and economic sustainability.

II. MATERIALS AND METHODS

The study draws on a rich corpus of official materials, including the UN Charter, the Act on Greenland Self-Government (2009), the treaties governing NATO's presence in the region (the 1951 Agreement), and EU strategic documents on combating economic coercion. Analyses by leading experts in polar law and international security, as well as reports by the US Space Force and the Danish government, are used. The main research methods include:

- Legal-normative method: To analyze the legitimacy of territorial claims in relation to jus cogens norms and the constitutional mechanisms of the Kingdom of Denmark.
- Institutional analysis: To assess the capacity of NATO and the EU to respond to the "alliance dilemma" and external pressure on critical infrastructure.
- Case studies: On the securitization of Greenlandic airports and resource competition with China to illustrate the practical dimensions of coercion.

For the purposes of the study, an interdisciplinary approach has been implemented, combining political science analysis with theories of international relations, game theory, "broken windows" theory, and concepts from the entrepreneurial ecosystem, such as Peter Thiel's concept of building the future "from zero to one".

III. RESULTS AND DISCUSSION

A. Historical context and the Monroe Doctrine as a framework for US "external" security

The US interest in Greenland is not an isolated diplomatic episode of the Trump administration era, but rather a manifestation of a long-term geostrategic constant, established since the early 19th century. At the heart of this relationship is the Monroe Doctrine (1823), which arose as a request for separate spheres of influence (America vs. Europe), the principles of non-colonization and non-intervention, and as a warning against European re-intervention in the New World. But in the 19th century, the doctrine underwent a significant evolution – from a defensive declaration against European colonialism to an instrument for consolidating American influence in the Western Hemisphere. Although historically addressed to Latin America, the doctrine became a broader strategic matrix, based on the idea that US security requires preventing a hostile military-political establishment in adjacent spaces, as well as in relation to key approaches to the continent [1], [2].

In the Bulgarian historiographical perspective, the Monroe Doctrine is often seen as the "symbolic capital" of American foreign policy. Even when the US formally avoids "European" conflicts, it considers it vital to prevent a hostile hegemony that would compromise the security of the American continent. It is significant that in the Bulgarian scholarly context the doctrine is used as an explanatory framework for Washington's perceptions of

strategic threats, including in periods of global competition [3], [4].

As Sexton [5, p. 5] points out, the doctrine became a flexible framework through which the US legitimized its territorial and economic ambitions, presenting them as a matter of national security. In this context, Greenland began to be seen not simply as a far northern territory, but as a strategic flank, control of which was essential to prevent foreign interference in the American sphere of influence.

It should also be noted that the interest in Greenland is not a "new topic" but has a long history that often "returns" to public debate in each more intense cycle of competition. The first official expression of this interest dates back to 1867, immediately after the purchase of Alaska and with the American discussions about the North Atlantic spaces that emerged during this period. The then Secretary of State William Seward commissioned a report that assessed Greenland's resources and its strategic location [6], [7, p. 263]. The government report "A Report on the Resources of Iceland and Greenland" (1868), prepared for the State Department, is indirect evidence that as early as the late 19th century, Washington viewed Iceland/Greenland as a resource and strategic asset in the North Atlantic arc [8]. On this basis, in this article we use the report as a starting point for an analysis that connects the assessment of resources with the geostrategic logic of the US for the North Atlantic and the Arctic.

The second key point is the 1946 offer, when the Harry Truman administration offered Denmark \$100 million in gold to purchase the island. The motive was dictated by the lessons of World War II, during which Greenland was de facto under American protection to prevent Nazi infiltration [9, pp. 9-10]. Copenhagen's refusal did not end US interest, but transformed it from a request for a territorial purchase to the construction of a large-scale military infrastructure. This can be clearly traced in the official diplomatic documentation of the period, which shows that the American side clearly argued the "vital importance" of Greenland for US security [10], [11]. Modern think tanks also recall this continuity and connect it to today's tensions in transatlantic relations [12].

The real transformation occurred during the Cold War, when the concept of the "Arctic as a geostrategic security multiplier" became dominant and the Arctic became an operational theater of strategic deterrence, as polar routes shortened the trajectories of strategic bombers and subsequently ballistic missiles. This "geographical advantage" turned Greenland into a frontline of the confrontation between NATO and the Warsaw Pact, and at the same time a key element of the northern defense architecture.

The transformation of the Arctic into a critical element of strategic deterrence led to the Greenland Defense Agreement (1951) between the United States and the Kingdom of Denmark, in the context of NATO, which also served as the legal basis for the American presence. Scholarly analysis of the negotiations reveals an

asymmetry of interests and “bargaining power” in the early Cold War context. Denmark sought collective defense and guarantees of sovereignty/legitimacy, while the United States insisted on operational freedom commensurate with the perceived threat [13]. In this sense, the text of the treaty (in publicly available archives) regulates the creation and use of “defense zones” and cooperation on the defense of the island [14]. The defense agreement thus signed between the United States and Denmark allows for the construction of the Thule Air Base (renamed Pituffik Space Base in 2023).

As noted in the analyses of a number of Bulgarian authors, the Arctic should be considered as a space for power projection, in which control over sea routes/communications and airspace becomes crucial for strategic competition and the balance of power [15], [16], [17, p. 49]. The Thule base is located 1200 km north of the Arctic Circle and is a critical element of the US Ballistic Missile Early Warning System (BMEWS). It serves as the “eyes of the North”, providing surveillance of outer space and protection against potential strikes through the North Pole – a route that remains the shortest route for intercontinental missiles between Russia and the US today [18], [19].

At the beginning of the 21st century, interest in Greenland was revived under the influence of climate change and the increased presence of Russia and China in the region. Modern American diplomacy revitalizes the idea that Greenland is America’s “Arctic gateway”. This is a clear indication that the Arctic is not “disappearing” from the strategic map, but attention is being reoriented due to a combination of: a) military-strategic competition; b) climate change and new routes; c) resource expectations; and d) technological transformation of defense (radar, space, communication systems). The American National Strategy for the Arctic Region (2022) explicitly places homeland security and defense, international law, and work with allies and partners among the leading interests [20].

The historical context shows that the dispute does not start with “one administration”, but relies on the logic of the northern flank of American security and on contractual-institutionalized mechanisms within NATO, which have been built for more than a century. The pressure for closer integration of the island into the economic and political sphere of the United States reflects the desire to limit Chinese investments in critical infrastructure (rare earth minerals and airports), and in analytical terms this can be interpreted as an “Arctic” update of the Monroe Doctrine [21], [22], [23]. Against this background, today’s political messages about “acquiring” Greenland can be interpreted as a radicalized rhetorical form of an older strategic intuition that control (or at least guaranteed access and operational freedom) over key northern strongholds reduces the risk of strategic surprise.

B. The legal dilemma: “Who owns Greenland?”

The question of Greenland’s belonging is often misunderstood through the prism of the classical sovereignty of the Kingdom of Denmark. In the contemporary legal architecture, however, the answer is

much more complex and is rooted in the dynamics between territorial integrity and the right to self-determination. This requires a precise balance between classical international law and the contemporary paradigm of indigenous rights. In this sense, we can point out that the “clash” is not only diplomatic, but also conceptual: between state-centric realism (the state as a territory that can be traded) and liberal legalism (the right of peoples to determine their own destiny) [24].

In international law, territory is not an object that is “owned” as private property, but a space over which a state exercises sovereignty and jurisdiction. This distinction is key when political actors come to the fore and talk about “buying” Greenland. In this sense, there is a transfer to public law of concepts inherent in private law and which are difficult to reconcile with modern norms of self-determination and territorial integrity. It is emblematic that as early as 1971, the International Law Commission (ILC) noted that the classic “cession” (including by purchase) was “increasingly obsolete” and its validity is today assessed through additional conditions, including consultation with the population.

The idea of purchasing Greenland draws on historical precedents such as the Louisiana Purchase (1803) [25] or Alaska (1867) [26]. These historical “territorial purchases” are classic examples of cession between states by treaty, in an era when international law treated territorial transfers much closer to the logic of a transaction and geopolitical exchange. In the era of decolonization and the establishment of the UN Charter, however, this transactional model is a legal anachronism. According to the principle of territorial integrity and the prohibition of the acquisition of territory by force (Article 2, paragraph 4 of the UN Charter), sovereignty is no longer a commodity. In this sense, political coercion through “offers to purchase” comes into direct conflict with Article 2(4) of the UN Charter, which prohibits the threat to the territorial integrity of any state.

The right to self-determination is a *jus cogens* norm in international law. It is both:

- a founding principle in the UN Charter (included as the UN’s purpose to develop friendly relations “on the basis of ... self-determination of peoples”) [28];
- a human right in the universal human rights covenants – in both the ICCPR and the ICESCR the first article begins with “All peoples have the right to self-determination” [29], [30].

The strongest contemporary legal argument against the idea that Greenland’s future can be decided “between capitals” is the 2009 Act on Greenland Self-Government. The regime’s practical legitimacy is strengthened by the fact that the Act on Self-Government itself was preceded by a referendum in 2008, in which some 75.5% supported the introduction of self-government [31], [32, p. 103].

The preamble to the Home Rule Act explicitly recognizes that the people of Greenland are “peoples under international law” with the right to self-determination [33].

And this is not just a political declaration, but is also reflected in Denmark's official notification to the UN Secretary-General [34]. In addition, Article 21 of the Home Rule Act itself is categorical that the decision on independence is made by the people of Greenland. If such a decision is made, negotiations follow between the Danish government and Naalakkersuisut (the government of Greenland), and the final agreement requires: the consent of the Inatsisartut (the parliament of Greenland), a referendum in Greenland and the consent of the Danish parliament [33].

Sovereignty over the territory currently belongs to the Kingdom of Denmark (within the state "Kingdom of Denmark/Realm", comprising Denmark, Greenland and the Faroe Islands) [31], [35]. This has also been confirmed within the framework of the UN, including through the adoption of the constitutional integration of Greenland in 1953 as an act of self-determination [36], [32]. An essential detail is that in the bilateral defense framework, the US has historically recognized Danish sovereignty over Greenland. The Greenland Defense Agreement (1951) explicitly speaks of US rights in "defense areas" "without prejudice" to the sovereignty of the Kingdom of Denmark [14]. In the context of the crisis, this has a double effect. On the one hand, it legally "anchors" the recognition of sovereignty, and on the other, politically it makes it even more difficult to legitimize claims for the transfer of sovereignty, especially if they are perceived as a threat or pressure.

Although Danish sovereignty remains the "legal envelope" of the territory, Denmark's domestic constitutional mechanism is designed to make the self-determination of Greenlanders a crucial condition for any change in status. This is why the claim that "Greenland can be bought" sounds like a conflict not only with political reality but also with positive law. In international law terms, this means that the legitimacy of any future change in status (independence, free association or integration elsewhere) in modern international law depends on the right to self-determination of the people of Greenland – i.e. on the democratically expressed will of the people in Nuuk and the rest of the island [33].

In this context, the purchase offer can be interpreted not as a business transaction, but as a form of geopolitical coercion that undermines the sovereign equality of states (Denmark) and the political will of recognized peoples (Greenlanders).

C. The geopolitical triangle: USA – Denmark – Greenland

If the legal dilemma determines who has the right to make decisions, the geoeconomic reality shows how those decisions are manipulated through investment. Greenland has become a testing ground for "soft power," where the struggle for rare earth elements and control of transportation infrastructure is used as a tool for geopolitical coercion.

The US proposal to "buy" Greenland (publicly articulated in 2019 and subsequently re-updated as political

pressure) acted as a catalyst that forced Copenhagen to rethink simultaneously: (a) the financial model of the relationship with Nuuk (from block grants to targeted infrastructure and social packages) and (b) the security architecture around the island (from a limited presence to accelerated investments in surveillance, maritime/air capabilities, and resilience of critical infrastructure). This is happening against the backdrop of three structural drivers of Arctic competition: Russian military resurgence, Chinese geoeconomic expansion, and climate transformation that is opening up new routes and making resources more accessible [37].

The Danish reaction begins with an almost textbook example of economic securitization – airports. The project to expand the airports in Nuuk and Ilulissat is "unspectacular" as a civil infrastructure, but it becomes geopolitically sensitive because, on the one hand, it is important for independence (tourism, connectivity), on the other, it is a symbol of defense coordination with the US and, last but not least, a potential point of Chinese influence. When the Chinese state-owned company China Communications Construction Group (CCCC) was proposed as the contractor, the US exerted unprecedented pressure on Denmark. In his article for SWP, Michael Paul explicitly describes how the Danish Prime Minister in 2018 proposed a package with a dual purpose: financing and reducing American fears of "excessive Chinese investment" [37]. The direct financial intervention from Copenhagen to block Chinese influence is defined by analyst Martin Breum as a turning point in the realization that infrastructure in the Arctic is a matter of national security, not just economics [38].

Another important aspect regarding China's geoeconomic expansion is related to the monopoly on rare earth elements. The melting ice sheet is opening up access to some of the world's largest deposits of rare earth elements (REE), critical for green energy and high-tech defense. The Kvanefeld project has become a symbol of this struggle. The Chinese company Shenghe Resources has acquired a significant stake in the project, which has raised concerns in Washington and Brussels. As an analysis by the Center for Strategic and International Studies (CSIS) points out, China is not simply seeking profit, but rather maintaining its global monopoly on the supply chain, using investments in Greenland as leverage against the West [39].

It should also be noted that after the failed rhetoric of buying the island (2019), the US strategy has shifted towards economic engagement. The report "America's Arctic Moment" emphasizes that in order to counter China's "Polar Silk Road" initiative, the US should invest in civilian projects that reduce Nuuk's dependence on external authoritarian capital [40, pp. 14, 35-36]. This turns economic aid into a tool for "defensive geopolitics." However, this U.S. framing should be considered in the context of China's official narrative.

China's official posture frames its Arctic engagement primarily through the language of international law, scientific cooperation, sustainable development, and connectivity. Within this narrative, the "Polar Silk Road"

is presented as an economic and logistical extension of broader connectivity policies rather than as a security project. The strategic tension, therefore, stems less from China's stated intentions and more from the structural effects of infrastructure finance: ports, airports, mining, and digital connectivity can generate long-term dependencies and dual-use concerns. This divergence explains why U.S. policy reads Chinese investments as a strategic lever and responds by "securitizing" civilian projects that would otherwise be treated as ordinary economic activity [41], [42].

From the perspective of American defense, the Arctic is the "northern approach" to the homeland and includes allied territories (Canada, Kingdom of Denmark/Greenland) where aerospace and maritime warning capabilities (NORAD) are located. The Pentagon's 2024 strategy describes the Arctic not only as a region for local defense, but also as an avenue for power projection to Europe and vital to transatlantic sea lines of communication [43].

For its part, Denmark is "rewriting" its vision of security from limited surveillance to a multi-domain presence. This is clearly evident from the Danish military modernization, which is developing in stages:

- 2021: Agreement on Arctic Capabilities – framed as a response to "increasing Russian activity and military build-up", with investments in radar, long-endurance drones, space surveillance and a ground station [44].
- 2025–2026: First/Second Agreement on the Arctic and North Atlantic – illustrates a qualitative leap in terms of strengthening security and defense: more Arctic ships (with icebreaking capability), maritime patrol aircraft with potential for anti-submarine missions, new radars (incl. East Greenland), an underwater cable in the North Atlantic and strengthening the Joint Arctic Command in Nuuk. It is important to note that the document links these investments directly to NATO and to the Greenland–Iceland–United Kingdom (GIUK) gap as an area for maritime situational awareness [45].

In parallel with all this, it should be noted that the Arctic governance environment is already fragmented after the invasion of Ukraine. Cooperation with Russia in the Arctic is at a standstill/on pause, and regional forums are finding it difficult to function fully – which increases the risk of misunderstandings and escalation [46]. And in this context, when a major ally (the United States) uses the rhetoric of territorial coercion, the result can be twofold: (a) political distrust between allies and (b) an incentive for Russia to exploit the rift informationally and operationally. In this regard, the example of increased military cooperation between the People's Republic of China (PRC) and Russia, including joint exercises in the Arctic, is indicative. In 2022 and 2023, ships of the PRC and the Russian Navy operated jointly in international waters off the coast of Alaska, and the Chinese Coast Guard and the Russian Federal Security Service signed a memorandum of understanding on the implementation of maritime law. These activities could

open the door for further Chinese presence in the Arctic and along the Northern Sea Route [43].

As a conclusion to the analysis, we can summarize that in the Arctic environment of competition and climate change, the idea of "buying" transforms the US-Denmark-Greenland triangle into an accelerator of changes that would otherwise be slower and technocratic. Denmark responds not only with a diplomatic "no", but with real money and capabilities.

D. NATO and EU – From "(non) zero-sum" game to the "zero to one" perspective for Greenland

If we use an analogy from the entrepreneurial ecosystem, linked to Peter Thiel's concept of building the future "from zero to one", we can try to change the way we think and act towards Greenland in the context of the new geopolitical and geo-economics realities. According to the technological entrepreneur, when something that already exists is upgraded and modified, the movement is from "one to n", while when something new, an innovation, is created, the movement is from "zero to one". He examines the concept in the context on the one hand of: technology, placing it in the vertical dimension of intensive progress, as it requires the creation of something that no one has done before, and on the other hand of: globalization, placing it in the horizontal or extensive dimension of progress, as it boils down to copying ideas that work [47].

To date, despite leading global players such as Russia, the United States, and China claim that they are creating a new world order, in practice, they are undermining the existing one established after World War II, shaped by the Bretton Woods system and the Cold War, and based on international law, liberal democracy, the market economy, and multilateral cooperation. Their actions, in fact, reproduce familiar patterns from the past such as the competition, instability, autocracy, protectionism, mistrust, and Hobbes' world of the war of "every man against every man". Thus, we are witnessing a return to the paradigms of realism and neorealism rather than constructive innovation in international relations that would lead to prosperity for humanity or, in particular, a better far-sightedly perspective for Russian, American, and/or Chinese citizens.

It appears that in the context of Greenland and the changed security environment, neither the zero-sum nor the non-zero-sum strategy has worked so far. The impact of climate change and rapid ice melt on the world's largest island lead to rapid opening of once-inaccessible shipping routes, lowering the cost and difficulty of extracting abundant natural resources, disrupting local wildlife and marine ecosystems, and reshaping the map in ways that increase human access – including for security and defense activities [48]. Another reason that is rarely mentioned among the motivating factors for the US are tech giants' and the wider digital economy's growing need for physical space and resources, related incl. to the Data centers that are experiencing an unprecedented surge in demand for energy, water and cooling, largely driven by the rapid growth of artificial intelligence, cloud computing and digital services. This factor matters because the "digital economy" has a material geography: data centres and AI

infrastructure require concentrated electricity supply, cooling, water, resilient cable connectivity, and a predictable regulatory environment, while their spatial concentration produces measurable infrastructure vulnerabilities and strategic dependencies [49]. Under Arctic conditions, climate and space can indeed generate comparative advantages for hosting compute capacity, yet they simultaneously turn the questions of “who finances, who builds, and who operates” into strategic issues of sovereign control, security standards, and long-term resilience. In this sense, Big Tech interest aligns with the broader securitization of infrastructure: decisions on digital projects are no longer merely economic, but increasingly embedded in policies designed to reduce external dependencies and constrain potential levers of influence—particularly in the wider context of competition around the “Polar Silk Road” [49]. Notably, Greenland has debated a foreign investment screening framework covering sensitive sectors, and the discussion has explicitly extended to large-scale investment proposals linked to digital infrastructure [50]. Consequently, Big Tech should be treated as an emerging non-state “power actor” that accelerates Greenland’s transformation into a critical node where security, infrastructure, and geoeconomic competition converge.

In the case of a non-zero-sum game, the parties’ interests align to produce mutual benefit – Denmark has control over constitutional matters, foreign policy, security and defense in Greenland, while the US has its bases and the opportunity to expand their scope. However, this “win-win” situation no longer satisfies the Trump administration due to the changing resource, geographic and transportation landscape, and he is signaling an intention to impose hard power.

In the potential case of zero-sum game, Greenland would become a potential new “battlefield” for nation states. An interesting fact is that of the so-called “Arctic Eight” (Canada, Russia, the US, Norway, Denmark, Finland, Sweden, Iceland), only Russia is not part of NATO. Without claiming to be exhaustive, potential points of tension outside the US-Denmark-Greenland triangle are as follows: 1) NATO could block Russia’s Baltic Fleet at the Skagerrak Strait, as was considered during the Cold War; 2) Tensions may arise between Norway and Russia in the Barents Sea. Norway has expressed claims over the Gakkel Ridge as an extension of its Exclusive Economic Zone, while Russia disputes these claims based on its own position regarding the northernmost territories on Earth, particularly the Svalbard (Spitsbergen) Islands. Although most states recognize Norwegian sovereignty, the growing presence of Russian migrants and the formation of a Russian community there could serve as a useful instrument for future Russian claims over all the Spitsbergen Islands; 3) Potential rivalry between the United States and Russia over the Bering Sea, the Arctic Ocean, and the northern Pacific; 4) Possible disagreements between the United States and Canada over offshore oil rights and access to the waters of the Canadian Arctic Archipelago; 5) A dispute between Canada and Denmark over Hans Island, located in the Nares Strait between

Greenland and Ellesmere Island. As the foreign policy expert and journalist Tim Marshall underlines – all disputes over sovereignty in Arctica stem from the same desires and fears, namely the desire to protect military and commercial shipping routes, the desire to control the region’s natural resources, and the fear that others may gain where you lose [51]. Among the Alliance’s member states, only the US has openly expressed intentions to violate NATO’s core logic, namely the protection of the sovereignty and territorial integrity of its members, which provoked the Danish prime minister Mette Frederiksen to question the future existence of NATO by underlining that: “everything would stop” in the event of a US attack on another NATO country; a US takeover of Greenland would mean the end of the NATO military alliance [52].

a) NATO and the “alliance dilemma”

The “Broken windows” theory of Wilson and Kelling (from 1982) argues that visible disorder in a neighborhood – like broken windows, graffiti, or loitering – signals neglect, creates fear, weakens social control, and ultimately leads to serious crime. The idea is that addressing signs of disorder early is a quicker, cheaper way to prevent larger crimes [53]. In classic broken windows theory, disorder comes from external neglect or low-level incivility that invites crime, but what if the windows are broken from the inside? In this way the logic changes as the source of disorder is not outsiders and this suggests erosion of trust from within, institutional failure, social controls weakening because people no longer believe in the system. The use of the metaphor as an analogy for the behavior of the US Trump’s administration in NATO, is intended to highlight signals indicating the need for a timely response to the actions of a member of the Alliance in order to prevent more serious consequences.

If the early signs of erosion are not addressed in time, the question will increasingly be raised whether a hypothetical “transfer of sovereignty” over Greenland would unravel the idea of a unified West and turn what some call “NATO 3.0” into something closer to the Warsaw Pact than to the Alliance’s original design [54]. For this reason, as a result of the US actions, on the one hand Denmark began with diplomatic shuttle efforts, and on the other hand - France, Germany, the UK, Norway, Netherlands and Sweden symbolically sent small contingents of troops to Greenland in a so-called a reconnaissance mission, in order to boost security and reinforce Danish sovereignty. The Danish-led joint exercises called Operation Arctic Endurance were seen by senior diplomat Olivier Poivre d’Arvor, as a mission which is sending a strong political signal: “This is a first exercise... we’ll show the US that NATO is present” [55].

In contrast to the Russia’s war against Ukraine, which has motivated traditionally neutral countries such as Finland and Sweden to join the Alliance in 2023 and 2024, by significantly strengthening the Northern Flank and the Arctic, the US, through its behavior towards Greenland and Denmark is creating vulnerability by undermining NATO’s security and weakening trust between allies. While, in October 2024, the Chair of NATO’s Military Committee

stated: “NATO will defend its interests in the Arctic. We have a responsibility to protect all our Allies, including the seven here in this region... and uphold the international rules-based order, which includes freedom of navigation” [56], today the allies are facing the so called “alliance dilemma” as the pressure from a leading ally distorts the logic of the collective defense. This dilemma, often referred to as the “abandonment-entrapment” dilemma, describes the central tension in security alliances where a state worries that its ally may fail to provide the promised protection (abandonment) or, conversely, that the partner or the alliance may pull it into an unwanted conflict (entrapment). Thus, the alliances require constant management of commitment levels and present a political relationships shaped by fear, bargaining, and perception. According to Glenn Snyder the alliances are not only about deterring enemies, they are also about managing anxieties between allies [57]. In this regard, preserving and respecting the principle of multilateralism and initiating a special NATO Arctic mission will help overcome the “alliance dilemma” through collective defense commitment as well as by creating a better perception of trust among the allies.

In their book “The Triangle of Power: Rebalancing the New World Order” and during the discussions in Davos, impacted by the Greenland issue, the Finnish president Stubb contrasted a “multipolar world”, driven by transactions, where countries focus on making deals, leveraging power and dividing spheres of influence reminiscent of the XIXth century, with a multilateral order based on strong institutions, rules, and norms – the model Finland supports and believes most countries favor [58]. In a joint statement, the Nordic foreign ministers of Denmark, Finland, Iceland, Norway and Sweden reaffirmed their commitment, as Arctic states and NATO allies, to: strengthening security, stability and cooperation in the Arctic; supporting increased NATO presence and investment in regional defense; stressing respect for fundamental principles of the UN Charter and international law, including the inviolability of borders; recalling Denmark’s long-standing defense cooperation with the US, and underlining that matters concerning Denmark and Greenland are for Denmark and Greenland alone to decide [59].

In the context of publicly declared intentions by US President Donald Trump to impose control over Greenland, the Prime Minister of Canada likewise outlined a new approach in his historic speech at the World Economic Forum in Davos, stating that: “a rupture in the world order ends a pleasant fiction and ushers in a harsh reality where major powers act without limits. Nevertheless, countries, especially middle powers like Canada, are not powerless and they can help build a new order grounded in human rights, sustainable development, solidarity, sovereignty, and territorial integrity. Carney emphasized the rules-based international order is fading and outlined how Canada was adapting through “value-based realism” by building strategic autonomy (being pragmatic) while maintaining values like human rights and sovereignty (being principled). He called for middle powers, such as his own,

to work together to counter the rise of hard power and the great power rivalry, in order to build a more cooperative, resilient world [60].

The reaction of the EU and other “middle powers” to such an approach would determine whether it will lead to “extensive” (to copy ideas from the past experience) or “intensive” (to embrace the innovativeness) progresses in the future. If the EU builds a true European Defense Union – being equipped with EU military and defense capabilities, having steadily independence from US armament and technologies as well as forces to safeguard its European sovereignty, so its dependence from United States, incl. in the framework of NATO, would be significantly diminished. This would also lead to a much stronger European pillar in the Alliance that could counterbalance a potential increase in the use of US hard power and to the strengthening of EU defense capabilities in the High North. At the same time, the institutionalisation of NATO’s role through a special NATO Arctic mission will help overcome the “alliance dilemma” and refocus attention on addressing the challenges of deterring Russian ambitions and continuously monitoring China’s growing interest, as well as on a farsighted pursuit of a “zero to one” perspective for Greenland.

b) EU, Greenland’s status vis-à-vis the Union and the Musketeer “one for all, all for one” principle

Greenland left the European Economic Community in 1985 after a 1979 home-rule referendum driven by fishing rights, becoming the first territory to withdraw and thereafter an EU Overseas Country and Territory associated through Denmark under the 1985 Greenland Treaty. Although no longer in the EU, Greenlanders remain Danish and thus EU citizens. Today, EU-Greenland relations, governed by the Greenland Treaty and the 2021 Overseas Association Decision, focus on fisheries, education, and increasingly green growth and sustainable raw materials, with €225 million allocated for 2021-2027, a proposed doubling for MFF 2028-2034, a new political visibility marked by an EU office in Nuuk (in March 2024) and a November 2023 MoU on sustainable raw materials value chains. Fisheries remain central through preferential market access linked to EU fishing rights, renewed in a 2025-2030 protocol, while Greenland also participates in EU programmes such as Horizon Europe, Erasmus+, InvestEU, and INTERREG [48].

Unlike NATO where the territory of Greenland is covered by article 5 and 6 of the North Atlantic Treaty, in the EU the territory is not part of it, so the mutual defense clause under article 42.7 TEU does not clearly apply, yet its people are citizens of the Union. In this regard, the Musketeer “one for all, all for one” principle in EU is reflected more in terms of economic and development instruments, investing in people, showing solidarity in addressing climate change and promoting multilateralism. The soft power actions of the EU in Greenland are of key importance for the stability and security of Greenland. Considering that the Greenland’s 31-seat parliament (Inatsisartut) includes the Democrats (social-liberal, cautious on independence – 10 seats), Naleraq (strongly

pro-independence – 8 seats.), Inuit Ataqatigiit (left-leaning, pro-independence – 7 seats), Siumut (social-democratic, pro-independence – 4 seats), and Atassut (conservative, pro-union with Denmark – 2 seats) [61], working closely with the local population and political parties, most of which support independence, is essential, as alongside threats of purchase, pressure, or coercive power, an additional front is opening in the form of cognitive warfare targeting the minds and hearts of local and Indigenous people by exploiting the trauma of the colonial past and its legacy's impact.

Greenland's internal political dynamics suggest that the debate over the U.S. presence and external pressure on the island is not binary ("for" or "against"), but is filtered through the interconnected issues of independence, economic resilience, and the terms of foreign investment. In this context, the positions of local political leaders and institutions operate as a "legitimacy filter": even when security arguments point toward a stronger transatlantic footprint, public acceptance remains conditional and politically contested – especially where pressure is perceived as constraining Greenlandic autonomy [62]. Public opinion data reinforces this point by indicating widespread rejection of scenarios involving accession to the United States, supporting the broader claim that any durable arrangement depends on local democratic legitimacy rather than externally imposed "deals" [63]. Consequently, the geopolitical triangle should be analysed not only through state strategies (U.S.–Denmark) but also through Greenland's domestic legitimization of security choices, which ultimately shapes their sustainability over time.

Adopted in October 2021 and undergoing renewal, the EU's Arctic Policy promotes peaceful cooperation, climate action and sustainable development, guided by priorities of protecting the climate and environment, supporting sustainable development, and promoting peace, stability and cooperation, with a strong focus on Indigenous Peoples, local communities and future generations, while its strengthened presence highlights education (90% of funding), renewable energy, biodiversity, sustainable tourism, research cooperation and critical raw materials as central to a partnership supporting Greenland's development [64], [65].

c) Tension in transatlantic solidarity and EU instruments against economic and political coercion

On 17 January US president Trump announced he would apply an extra 10% tariff on Denmark the UK and six other European countries (Finland, France, Germany, The Netherlands, Norway, and Sweden). This would begin on 1 February, and increase to 25% on 1 June 2026. The tariffs he said would apply "until such time as a Deal is reached for the Complete and Total purchase of Greenland". He said he was applying tariffs to these countries because they had "journeyed to Greenland, for purposes unknown", that this was "a very dangerous situation for the Safety, Security, and Survival of our Planet", and that "these Countries, who are playing this very dangerous game, have put a level of risk in play that

is not tenable or sustainable" [62]. In a joint statement on January 18, the EU countries Denmark, Finland, France, Germany, the Netherlands and Sweden, together with Norway and the United Kingdom affirmed their commitment as NATO members to strengthening Arctic security, as a shared transatlantic interest, through the pre-coordinated Danish exercise with Allies, expressed full solidarity with the Kingdom of Denmark and the people of Greenland, stood ready to engage in dialogue based on the principles of sovereignty and territorial integrity, warned that tariff threats risk a dangerous downward spiral in transatlantic relations, and affirmed they are committed to upholding their sovereignty [66].

The European Union, for its part, also expressed its support for Denmark and Greenland through its supranational institutions, with the Presidents of the European Commission and the European Council issuing a joint statement where they emphasized that: territorial integrity and sovereignty are fundamental principles of international law essential for Europe and the wider international community, and while the EU underscores its shared transatlantic interest in Arctic peace and security through NATO, supports the pre-coordinated Danish exercise with allies, stands in full solidarity with Denmark and Greenland, and calls for continued dialogue with the US, it warns that tariffs would damage transatlantic relations and reaffirms Europe's unity and commitment to its sovereignty [67]. In addition, the European Commission president von der Layen underlined in Davos speech that "EU response will be unflinching, united and proportional" to US tariffs, in full solidarity with Denmark [68]. Informally, voices were heard calling also for the EU's "trade bazooka". The Anti-Coercion Instrument, which entered into force on 27 December 2023, enables the EU to deter and, if necessary, respond to situations where a third country seeks to pressure the European Union or a Member State into making a particular choice by applying or threatening measures affecting trade or investment, allowing the European Commission, after examination, a Council determination, and efforts at dialogue, to adopt response measures such as restrictions on access to the EU Single market, in line with public international law [69].

As a result of the messages and actions of the Arctic countries in NATO, the European institutions, and the potential of the Anti-coercion toolbox protecting the EU and its Member States from third countries' economic coercion, President Trump has softened his tone and abandoned plans to raise tariffs. On 21 January during a speech to the World Economic Forum in Davos, President Trump said: "I don't want to use force. I won't use force. All the US is asking for is a place called Greenland. You can say yes, and we will be very appreciative. Or you can say no and we will remember." He also called for "immediate negotiations to once again discuss the acquisition of Greenland by the United States". Later that day, following discussions with NATO Secretary General Mark Rutte, Mr Trump announced he would no longer be imposing the tariffs after "a very productive meeting" in which they "formed the framework of a future deal with respect to Greenland and (...) the entire Arctic Region"

[62]. Thus, at the informal meeting of the members of the European Council, 22 January 2026 on recent developments in transatlantic relations and their implications for the EU, President Costa stressed that the EU and US share interests in the Arctic through NATO, affirmed the EU's stronger role in the region, stressed that only Denmark and Greenland can decide their affairs, and reiterated the EU's commitment to the principles of international law, territorial integrity and national sovereignty [70].

Although the European Union understands the laws of physics, it also knows the lessons of history. For this reason, it would apply Newton's third law in international affairs with great caution. The EU tries to lead by example, namely by promoting multilateralism, which is part of its DNA.

IV. CONCLUSIONS AND SUMMARY

The analysis of the current situation around Greenland allows us to make a systematic assessment of the risks and derive strategic recommendations for dealing with the crisis. The main risk lies in the fragmentation of the Arctic governance environment and the potential use of the rhetoric of territorial coercion to undermine allied confidence in NATO. Increased military cooperation between Russia and China in international waters off Alaska and along the Northern Sea Route creates the risk of strategic surprise and operational exploitation of political rifts between Western partners. In parallel, economic vulnerability from "excessive" external investments in critical infrastructure and the monopoly on rare earth elements require immediate countermeasures to protect sovereign equality.

In this regard, from an academic and strategic perspective, we would outline the following recommendations:

- Institutionalizing NATO's role in the Arctic: Formalizing collective defense mechanisms in Greenland through a specialized mission to ensure security without compromising Danish sovereignty and Greenlandic self-government. Due to the rapidly evolving nature of the issue, it is worth noting that a recommendation advanced in this article was effectively overtaken by events, as NATO launched the specialized mission "Arctic Sentry" to increase its military presence in Greenland while the paper was being prepared. Nevertheless, the recommendations for strengthening NATO's European pillar, preventing the "alliance dilemma", promptly addressing signals of disorder and "window breaking" within the Alliance itself, and preventing erosion of trust among allies towards US remain valid.

- Activating EU instruments for economic, educational, and sustainable development and resilience-building: Using the EU's Anti-Coercion Instrument to support Greenland in negotiations for strategic resources and protection from external pressure. Even though cautious in applying Newton's law, the EU has a "trade bazooka" at its disposal to deliver a proportionate response. Doubling the funding for education, sustainable development, economic

diversification, climate and cognitive security in the next EU budget post 2027 is also necessary. The cognitive battlefield and FIMI should not be underestimated, as although they are under the "military radar", they create conditions for polarization in the European democratic societies. Given that the majority of parties in the Inatsisartut want independence, which would happen through a referendum, and in light of the colonial legacy of the Indigenous population, which is often invoked by third countries, With the support of the EU, Greenland should enhance its resilience in anticipation of an additional front of geopolitical and hybrid challenges.

- Prioritizing the right to self-determination: Any change in the security architecture or the status of the island must be firmly based on the democratic will of the people of Nuuk, as enshrined in the 2009 Act of Self-Government.

Greenland is extremely well suited for demonstrating an innovative approach in a "zero to one" perspective and the international players have the historical chance to show up. As Tim Marshall emphasizes through the lens of "Prisoners of Geography", conflicts often begin from fear and greed, but the Arctic may be different. History shows that when one side gains, another usually loses, shaped by geography and human nature. However, technology has helped us overcome geographic limits. In today's globalised world, we can use this progress to ensure the Arctic benefits everyone, overcoming our more exploitative instincts and turning this "great game" into a shared good [51]. The global community needs creativity, strategic empathy towards humanity, and an innovative approach more than ever before, because, as Sir Ken Robinson teaches us the creativity is the process of developing original ideas with value [71]. Innovation is the process of putting new ideas into practice, and one potential such idea is the "zero to one" perspective for Greenland.

In conclusion, the crisis surrounding Greenland is a litmus test for the sustainability of the international legal order and the ability of Western institutions to adapt to the new geopolitical reality. It proves that in the modern world, territory is not a commodity that can be bought or sold, but a sovereign space whose legitimacy is rooted in human rights and the will of the population. The future stability of the Arctic depends on the synchrony between NATO's military power and the EU's political and legal protection, which together must ensure that the region remains a space of law, not geopolitical coercion. Greenland remains the key front on which to decide whether the principle of sovereign equality will prevail over narrow realism.

REFERENCES

- [1] U.S. Department of State, "Milestones: The Monroe Doctrine, 1823," [history.state.gov](https://history.state.gov/milestones/1801-1829/monroe). [Online]. Available: <https://history.state.gov/milestones/1801-1829/monroe>. [Accessed: Feb. 2, 2026].
- [2] National Archives, "Monroe Doctrine (1823)," May 10, 2022. [Online]. Available: <https://www.archives.gov/milestone-documents/monroe-doctrine>. [Accessed: Feb. 2, 2026].
- [3] P. Petkov, "The USA and Bulgaria, 1917–1918," Yearbook of Sofia University "St. Kliment Ohridski" – Faculty of History (orig. in Bulgarian: „Годишник на Софийския университет „Св. Климент Охридски“ – Исторически факултет“), vol. 73,

- no. 1, pp. 61–107, 1982, <https://doi.org/10.60053/GSU.IF.1.73.61-107>. [Online]. Available: <https://annual.uni-sofia.bg/index.php/hist/article/view/1284>. [Accessed: Feb. 2, 2026].
- [4] P. Petkov, “The United States and the First World War: The Peace Program of President Woodrow Wilson,” Yearbook of Sofia University “St. Kliment Ohridski” – Faculty of History (orig. in Bulgarian: „Годишник на Софийския университет „Св. Климент Охридски“ – Исторически факултет“), vol. 90, no. 1, pp. 115–184, Nov. 2000, <https://doi.org/10.60053/GSU.IF.1.90.115-184> [Online]. Available: <https://annual.uni-sofia.bg/index.php/hist/article/view/1224>. [Accessed: Feb. 2, 2026].
- [5] J. Sexton, *The Monroe Doctrine: Empire and Nation in Nineteenth-Century America*. New York, NY, USA: Hill and Wang, 2011. [Online]. Available: https://books.google.co.ve/books?id=u4GVKXN8SWYC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. [Accessed: Feb. 2, 2026].
- [6] O. Godeanu-Kenworthy, “American Attempts at Northern Expansion in the 19th Century,” Nordics.info, Mar. 31, 2025. [Online]. Available: <https://nordics.info/nnl/show/artikel/american-attempts-at-northern-expansion-in-the-19th-century>. [Accessed: Feb. 2, 2026].
- [7] B. Dyer, “Robert J. Walker on Acquiring Greenland and Iceland,” The Mississippi Valley Historical Review, vol. 27, no. 2, pp. 263–266, Sep. 1940, <https://doi.org/10.2307/1896815>. [Accessed: Feb. 2, 2026].
- [8] U.S. Department of State, *A Report on the Resources of Iceland and Greenland*, B. M. Peirce, Comp. U.S. Government Printing Office, 1868. [Online]. Available: <https://books.google.bg/books?id=U9IIAAAAMAAJ&printsec=frontcover&hl=bg#v=onepage&q&f=false>. [Accessed: Feb. 2, 2026].
- [9] H. A. Conley, M. Melino, N. Tsafos, and I. Williams, *America’s Arctic Moment: Great Power Competition in the Arctic to 2050*. Washington, DC, USA: Center for Strategic and International Studies (CSIS), 2020. [Online]. Available: <https://www.csis.org/analysis/americas-arctic-moment-great-power-competition-arctic-2050>. [Accessed: Feb. 2, 2026].
- [10] U.S. Department of State, Office of the Historian, “Memorandum by the Joint Chiefs of Staff to the Secretary of State: Over-all examination of U.S. requirements for military bases and rights” (Doc. 580, Nov. 7, 1945), in *Foreign Relations of the United States, 1946, General*; The United Nations, vol. 1, R. R. Goodwin, N. H. Petersen, M. W. Kranz, and W. Slany, Eds. Washington, DC, USA: U.S. Government Printing Office, 1972, pp. 1113–1117. [Online]. Available: <https://history.state.gov/historicaldocuments/frus1946v01/d580>. [Accessed: Feb. 2, 2026].
- [11] U.S. Department of State, Office of the Historian, “Conversation with Danish Foreign Minister Gustav Rasmussen emphasizing the vital importance of Greenland” (Telegram 811.24559B/1–247), *Foreign Relations of the United States (FRUS), 1947, vol. III, Doc. 414, 1947*. [Online]. Available: <https://history.state.gov/historicaldocuments/frus1947v03/d414>. [Accessed: Feb. 2, 2026].
- [12] M. Weller, “Who owns Greenland?,” Chatham House, Jan. 9, 2026. [Online]. Available: <https://www.chathamhouse.org/2026/01/who-owns-greenland>. [Accessed: Feb. 2, 2026].
- [13] N. Petersen, “Negotiating the 1951 Greenland Defense Agreement: Theoretical and empirical aspects,” *Scandinavian Political Studies*, vol. 21, no. 1, 1998. [Online]. Available: https://tidsskrift.dk/scandinavian_political_studies/article/view/32916. [Accessed: Feb. 2, 2026].
- [14] Yale Law School, Avalon Project, “Defense of Greenland: Agreement between the United States and the Kingdom of Denmark,” Apr. 27, 1951. [Online]. Available: https://avalon.law.yale.edu/20th_century/den001.asp. [Accessed: Feb. 2, 2026].
- [15] P. Georgiev, “The Battle for the North Pole: The New Arctic Geopolitics,” *Geopolitika* (orig. in Bulgarian: „Битката за Северния полюс: новата арктическа геополитика“), Apr. 17, 2014. [Online]. Available: <https://geopolitika.eu/spisanie-geopolitika/129-2014/broi-1-2014/2005-bitkata-za-severniya-polyus-novata-arkticheska-geopolitika>. [Accessed: Feb. 2, 2026].
- [16] N. Stefanov, “The Military Dimensions of the New Battle for the Arctic,” *Geopolitika* (orig. in Bulgarian: „Военните измерения на новата битка за Арктика“), Jun. 28, 2020. [Online]. Available: <https://geopolitika.eu/2020/183-broy-3-2020/3203-voennite-izmereniya-na-novata-bitka-za-arktika>. [Accessed: Feb. 2, 2026].
- [17] I. Sotirov, “Military-strategic conditions of stability in international relations,” in *110 Years of Tradition, Quality, Prestige: Proceedings of the Annual Scientific Conference – Part I* (Apr. 12–13, 2022, Sofia, Bulgaria) (orig. in Bulgarian: „Военностратегически условия на стабилността в международните отношения,“ в „110 години традиция, качество, престиж: Сборник доклади от годишна научна конференция – Част I“), pp. 46–54. Sofia, Bulgaria: G. S. Rakovski National Defence College, 2022. [Online]. Available: <https://rmdc.bg/wp-content/uploads/2023/03/1-2-%D0%A%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F-06-10-2022-300.pdf>. [Accessed: Feb. 2, 2026].
- [18] United States Space Force, “Thule Air Base Gets New Name,” Apr. 6, 2023. [Online]. Available: <https://www.spaceforce.mil/news/article/3355840/thule-air-base-gets-new-name/>. [Accessed: Feb. 2, 2026].
- [19] J. Hirsch, “Challenging our conventional thinking in the Arctic,” *Journal of Arctic and Climate Security Studies*, vol. 1, no. 1, 2023. [Online]. Available: https://tedstevensarcticcenter.org/wp-content/uploads/2023/09/JACSS-Vol-1.-No.-1-20230906_revised_20230911_1936AKDT.pdf. [Accessed: Feb. 2, 2026].
- [20] The White House, *National Strategy for the Arctic Region*. 2022. [Online]. Available: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Strategy-for-the-Arctic-Region.pdf>. [Accessed: Feb. 2, 2026].
- [21] M. Lanteigne, “Greenland’s Airport Saga: Enter the US?,” *Over the Circle*, Sep. 18, 2018. [Online]. Available: <https://overthecircle.com/2018/09/18/greenlands-airport-saga-enter-the-us/>. [Accessed: Feb. 2, 2026].
- [22] M. Lanteigne and M. Shi, “‘No Sale’: How Talk of a US Purchase of Greenland Reflected Arctic Anxieties,” *Over the Circle*, Sep. 17, 2019. [Online]. Available: <https://overthecircle.com/2019/09/17/no-sale-how-talk-of-a-us-purchase-of-greenland-reflected-arctic-anxieties/>. [Accessed: Feb. 2, 2026].
- [23] C. Edwards, “The ‘Donroe Doctrine’ reaches the Arctic,” *International Institute for Strategic Studies (IISS)*, Jan. 12, 2026. [Online]. Available: <https://www.iiiss.org/online-analysis/online-analysis/2026/01/the-donroe-doctrine-reaches-the-arctic/>. [Accessed: Feb. 2, 2026].
- [24] In classical geopolitics (realism), Greenland is seen as an “object” – a territory that can be bought, sold or used for military purposes because a stronger state has an interest in doing so (so-called Realpolitik). Realpolitik does not necessarily deny law or values, but views them as secondary interests and strong realities (especially in times of crisis). Liberal legalism rejects this. It argues that they are not free to make any demands now because they are constrained by international treaties and legal norms. According to this logic, even the richest country (the USA) cannot simply “buy” an island because there are legal procedures and rights of the population that are above market logic.
- [25] International Law Commission, “Fourth report on succession of States in respect of matters other than treaties,” U.N. Doc. A/CN.4/247, 1971. [Online]. Available:

- https://legal.un.org/ilc/documentation/english/a_cn4_247.pdf. [Accessed: Feb. 3, 2026].
- [26] United States of America and the French Republic, "Treaty between the United States of America and the French Republic (Louisiana Purchase Treaty)," Apr. 30, 1803. [Online]. Available: https://avalon.law.yale.edu/19th_century/louis1.asp. [Accessed: Feb. 3, 2026].
- [27] United States of America and Russia, "Treaty concerning the Cession of the Russian Possessions in North America (Alaska Treaty of Cession)," Mar. 30, 1867. [Online]. Available: <https://www.govinfo.gov/content/pkg/STATUTE-15/pdf/STATUTE-15-Pg539.pdf>. [Accessed: Feb. 3, 2026].
- [28] United Nations, Charter of the United Nations and Statute of the International Court of Justice, 1945. [Online]. Available: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>. [Accessed: Feb. 3, 2026].
- [29] OHCHR, "International Covenant on Civil and Political Rights (ICCPR)," 1966. [Online]. Available: <https://www.ohchr.org/en/instruments-mechanisms/instruments/internationalcovenant-civil-and-political-rights>. [Accessed: Feb. 3, 2026].
- [30] OHCHR, "International Covenant on Economic, Social and Cultural Rights (ICESCR)," 1966. [Online]. Available: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>. [Accessed: Feb. 3, 2026].
- [31] Denmark (Statsministeriet), "Greenland." [Online]. Available: <https://english.stm.dk/the-primeministers-office/the-unity-of-the-realm/greenland/>. [Accessed: Feb. 3, 2026].
- [32] K. Göcke, "The 2008 referendum on Greenland's autonomy and independence: Implications for the future of Greenland's international legal status," *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, vol. 69, no. 1, pp. 103–122, 2009. [Online]. Available: https://www.zaoerv.de/69_2009/69_2009_1_a_103_122.pdf. [Accessed: Mar. 2, 2026].
- [33] Denmark (Statsministeriet), "Act No. 473 of 12 June 2009 on Greenland Self-Government (English translation)," 2009. [Online]. Available: <https://english.stm.dk/media/4vgewyoh/gl-selvstyrelse-uk.pdf>. [Accessed: Feb. 3, 2026].
- [34] Statsministeriet, "Notifikation af 7. oktober 2009 til FN's generalsekretær om selvstyreløven [Notification of 7 October 2009 to the UN Secretary-General concerning the Self-Government Act]," Oct. 7, 2009. [Online]. Available: <https://www.stm.dk/media/zbalffp3/10-notifikation-af-7-oktober-2009-til-fn-s-generalsekretær-om-selvstyreløven.pdf>. [Accessed: Feb. 2, 2026].
- [35] Denmark (Statsministeriet), "The Unity of the Realm." [Online]. Available: <https://english.stm.dk/the-prime-ministers-office/the-unity-of-the-realm/>. [Accessed: Feb. 3, 2026].
- [36] UN General Assembly, "Resolution 849 (IX): Cessation of the transmission of information under Article 73 e of the Charter in respect of Greenland," 1954. [Online]. Available: <https://www.refworld.org/legal/resolution/unga/1954/en/85064>. [Accessed: Feb. 4, 2026].
- [37] M. Paul, "Arctic Repercussions of Russia's Invasion," SWP Comment, 2022. [Online]. Available: <https://www.swp-berlin.org/10.18449/2021C10/>. [Accessed: Feb. 4, 2026].
- [38] M. Breum, "How a dispute over China and Greenland's airports worked its way toward a solution," *Arctic Today*, Jun. 30, 2018. [Online]. Available: <https://www.arctictoday.com/dispute-china-greenlands-airports-worked-way-toward-solution/>. [Accessed: Feb. 4, 2026].
- [39] M. Schwartz and G. Baskaran, "Greenland, Rare Earths, and Arctic Security," Center for Strategic and International Studies (CSIS), Jan. 8, 2026. [Online]. Available: <https://www.csis.org/analysis/greenland-rare-earths-and-arctic-security>. [Accessed: Feb. 4, 2026].
- [40] H. A. Conley and M. Melino, *America's Arctic Moment: Great Power Competition in the Arctic to 2050*. Washington, DC, USA: Center for Strategic and International Studies (CSIS), 2020. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Conley_ArcticMoment_layout_WEB%20FINAL.pdf. [Accessed: Feb. 5, 2026].
- [41] The State Council Information Office of the People's Republic of China, "China's Arctic Policy," White Paper, Jan. 2018. [Online]. Available: https://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm. [Accessed: Apr. 30, 2026].
- [42] Y. Hong, "China's Arctic policy on the basis of international law: Identification, goals, principles and positions," *Marine Policy*, vol. 100, pp. 265–276, Feb. 2019. doi: 10.1016/j.marpol.2018.11.027. [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0308597X18301982>. [Accessed: Apr. 30, 2026].
- [43] U.S. Department of Defense, 2024 Arctic Strategy, Jun. 21, 2024. [Online]. Available: <https://media.defense.gov/2024/Jul/22/2003507411/-1/-1/0/DOD-ARCTIC-STRATEGY-2024.PDF>. [Accessed: Feb. 5, 2026].
- [44] Danish Ministry of Defence, "Agreement on Arctic capabilities (Unofficial translation)," Feb. 11, 2021. [Online]. Available: <https://www.fmn.dk/globalassets/fmn/dokumenter/nyheder/2021/-agreement-on-arctic-capabilities-uk-.pdf>. [Accessed: Feb. 5, 2026].
- [45] Danish Ministry of Defence, "Fact sheet: Second Agreement on the Arctic and North Atlantic (Under the 2024–2033 Defence Agreement)," Oct. 10, 2025. [Online]. Available: <https://www.fmn.dk/globalassets/fmn/dokumenter/2025/-publikation-om-delaftale-2-om-arktisk-og-nordatlanten-eng-.pdf>. [Accessed: Feb. 5, 2026].
- [46] M. Paul, "Arctic repercussions of Russia's invasion: Council on pause, research on ice and Russia frozen out," *Stiftung Wissenschaft und Politik (SWP)*, SWP Comment no. 39/2022, Jun. 2022. [Online]. Available: https://www.swp-berlin.org/publications/products/comments/2022C39_ArcticAndRussiasInvasion.pdf. [Accessed: Feb. 6, 2026].
- [47] P. Thiel and B. Masters, *Zero to One: Notes on Startups, or How to Build the Future*. London, U.K.: Virgin Books, 2014.
- [48] G. Leclerc, *Greenland: Caught in the Arctic Geopolitical Contest*, European Parliamentary Research Service (EPRS), Members' Research Service, Briefing PE 769.527, Oct. 2025. [Online]. Available: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769527/EPRS_BRI\(2025\)769527_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769527/EPRS_BRI(2025)769527_EN.pdf). [Accessed: Feb. 9, 2026].
- [49] International Energy Agency, *Energy and AI*. Paris, France: IEA, 2025. [Online]. Available: <https://www.iea.org/reports/energy-and-ai>. [Accessed: May 4, 2026].
- [50] A. Jacobsen and T. Stonestreet, "Wary of U.S. investors, Greenland lawmakers push to pass foreign investment screening law," *Reuters*, Feb. 26, 2026. [Online]. Available: <https://www.reuters.com/world/europe/wary-us-investors-greenland-lawmakers-push-pass-foreign-investment-screening-law-2026-02-26/>. [Accessed: May 4, 2026].
- [51] T. Marshall, *Prisoners of Geography* (Bulgarian ed.: Пленници на географията). Sofia, Bulgaria: Knigomania, 2023.
- [52] F. Bahgat and S. D. Inayatullah, "NATO could end if US takes over Greenland – Danish PM," *Deutsche Welle*, Jan. 6, 2026. [Online]. Available: <https://www.dw.com/en/nato-could-end-if-us-takes-over-greenland-danish-pm/a-75401270>. [Accessed: Feb. 9, 2026].
- [53] A. J. McKee and The Editors of Encyclopaedia Britannica, "Broken windows theory," in *Encyclopaedia Britannica*. [Online]. Available: <https://www.britannica.com/topic/broken-windows-theory>. [Accessed: Feb. 9, 2026].
- [54] X. Heqian, "In Depth: Finland's Stubb warns world order at a crossroads," *Global Neighbours*, Feb. 2, 2026. [Online]. Available: <https://www.globalneighbours.org/in-depth-finlands-stubb-warns-world-order-at-a-crossroads/>. [Accessed: Feb. 9, 2026].

- [55] P. Kirby, "European military personnel arrive in Greenland as Trump says US needs island," BBC News, Jan. 15, 2026. [Online]. Available: <https://www.bbc.com/news/articles/cd0ydvxpejo>. [Accessed: Feb. 9, 2026].
- [56] NATO, "NATO will defend Allied interests in the Arctic says Chair of NATO Military Committee," Oct. 21, 2024. [Online]. Available: <https://www.nato.int/en/news-and-events/articles/news/2024/10/21/nato-will-defend-allied-interests-in-the-arctic-says-chair-of-nato-military-committee>. [Accessed: Feb. 9, 2026].
- [57] G. H. Snyder, *Alliance Politics*. Ithaca, NY, USA: Cornell University Press, 1997.
- [58] A. Stubb and M. Leonard, "How can we cooperate in a more contested world? Rebalancing the New World Order," World Economic Forum Annual Meeting 2026, Jan. 22, 2026. [Online]. Available: <https://www.weforum.org/meetings/world-economic-forum-annual-meeting-2026/sessions/rebalancing-the-new-world-order/>. [Accessed: Feb. 9, 2026].
- [59] Norwegian Government, "Joint statement by the foreign ministers of Denmark, Finland, Iceland, Norway and Sweden on 6 January 2026," Jan. 6, 2026. [Online]. Available: <https://www.regjeringen.no/en/whats-new/joint-statement-by-the-foreign-ministers-of-denmark-finland-iceland-norway-and-sweden-on-6-january-2026/id3145218/>. [Accessed: Feb. 9, 2026].
- [60] World Economic Forum, "Davos 2026: Special address by Mark Carney, Prime Minister of Canada," Jan. 20, 2026. [Online]. Available: <https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada/>. [Accessed: Feb. 9, 2026].
- [61] Arctic Portal, "Greenlanders have voted – major changes ahead?," Mar. 12, 2025. [Online]. Available: <https://arcticportal.org/ap-library/news/3707-greenlanders-have-voted-major-changes-ahead>. [Accessed: Feb. 9, 2026].
- [62] J. Curtis and S. Fella, "President Trump and Greenland: Frequently Asked Questions," House of Commons Library Research Briefing CBP-10472, Jan. 23, 2026. [Online]. Available: <https://commonslibrary.parliament.uk/research-briefings/cbp-10472/>. [Accessed: Feb. 9, 2026].
- [63] T. Paternoster and J. Liboreiro, "Most Greenlanders oppose joining US despite Trump's push, poll shows," *Euronews*, Jan. 29, 2025. [Online]. Available: <https://www.euronews.com/2025/01/29/most-greenlanders-oppose-joining-us-despite-trumps-push-poll-shows>. [Accessed: Apr. 30, 2026].
- [64] European External Action Service, "The EU in the Arctic: The EU's Arctic Policy." [Online]. Available: https://www.eeas.europa.eu/eeas/eu-arctic_en. [Accessed: Mar. 2, 2026].
- [65] European Commission, Multiannual Indicative Programme 2021–2027 for Greenland, Mar. 8, 2022. [Online]. Available: https://international-partnerships.ec.europa.eu/document/download/5f56a51b-7c23-4ba3-89b8-c14bf535c789_en?filename=mip-2021-c2021-9159-greenland-annex_en.pdf. [Accessed: Feb. 9, 2026].
- [66] Government Offices of Sweden, "Statement by Denmark, Finland, France, Germany, the Netherlands, Norway, Sweden and the United Kingdom," Jan. 18, 2026. [Online]. Available: <https://www.government.se/statements/2026/01/statement-by-denmark-finland-france-germany-the-netherlands-norway-sweden-and-the-united-kingdom/>. [Accessed: Feb. 9, 2026].
- [67] European Council, "Joint statement by President Costa and by President von der Leyen on Greenland," Jan. 17, 2026. [Online]. Available: <https://www.consilium.europa.eu/en/press/press-releases/2026/01/17/joint-statement-by-president-costa-and-by-president-von-der-leyen-on-greenland/>. [Accessed: Feb. 9, 2026].
- [68] S. Starcevic and C. Gijs, "Von der Leyen vows 'unflinching' response to Trump with EU-US relations in turmoil," *Politico*, Jan. 20, 2026. [Online]. Available: <https://www.politico.eu/article/europe-faces-permanent-new-world-order-greenland-ursula-von-der-leyen-says/>. [Accessed: Feb. 9, 2026].
- [69] European Commission, "Protecting against coercion: The Anti-Coercion Instrument for protecting the EU and its Member States from third countries' economic coercion," Dec. 27, 2023. [Online]. Available: https://policy.trade.ec.europa.eu/enforcement-and-protection/protecting-against-coercion_en. [Accessed: Feb. 9, 2026].
- [70] European Council, "Informal meeting of the members of the European Council, 22 January 2026." [Online]. Available: <https://www.consilium.europa.eu/en/meetings/european-council/2026/01/22/>. [Accessed: Feb. 9, 2026].
- [71] K. Robinson, *Out of Our Minds: Learning to Be Creative*, 2nd ed. Chichester, U.K.: Capstone Ltd., 2011.

Comparative Analysis of the National Security Strategies of Bulgaria, the USA, Russia and China Through the Prism of Key Security Theories

Daniel Berchev

Security and Defense Faculty
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
dberchev@nvu.bg

Abstract – In the context of accelerated geopolitical confrontation, militarization of technology, and the “extension” of security to economic, cyber, and societal dimensions, the study of different national security strategies allows us to understand not only what states say in their strategies, but also why they say it. This is critically important for security decision-makers as it will help them anticipate potential conflicts or areas of cooperation, recognizing when a state is acting out of fear (realism), when out of ideology (constructivism), and when out of pragmatic interest (liberalism). The analysis in this report focuses on examining the similarities and differences between the national security strategies of Bulgaria, the United States, Russia, and China, refracted through the prism of the key security theories: realism/neorealism, liberalism/neoliberalism, constructivism, and the Copenhagen School. Each of the countries mentioned is of a different caliber and geopolitical weight, but the choice is not accidental. The United States, Russia, and China represent the three main “power centers” of the modern world, and Bulgaria is the analytical “prism” through which to see how global tremors are felt at the local level.

The study is based on a review of official national security strategy documents and related doctrinal and sectoral policies in the areas of defense, cybersecurity, and international/foreign policy. The analysis integrates contemporary scholarly insights into the transformation of operational art and hybrid operations, emphasizing the need for doctrinal adaptability and theoretical clarity in a context of increasing strategic uncertainty.

Keywords – geopolitical rivalry, national security strategy, security theories

I. INTRODUCTION

The contemporary strategic environment is characterized by a simultaneous “expansion” of the

security agenda and the restoration of sovereignty as the guiding framework for legitimizing policies. In the Updated National Security Strategy of the Republic of Bulgaria of 2018, this is visible through the explicit derivation of citizen security and “human security” as the “true meaning” of national security, combined with the protection of sovereignty, territorial integrity and the state border [1]. Donald Trump’s version of the 2025 US National Security Strategy emphasizes the “critically necessary” link between ends and means and links national security to border control, industrial base, supply chains, and technological competitiveness, including in areas such as AI [2]. Russia’s 2021 strategy defines national security as a “state of protection” of national interests and explicitly describes information and space as new spheres of military action [3]. The Chinese White Paper (2025) frames security as “comprehensive, systematic, and relative,” emphasizing the “double-edged” effect of the scientific and technological revolution and explicitly including emerging risks in cyberspace and other “emerging fields” [4].

This combination of state-centric sovereignty, technological and economic vulnerability, and sectoral expansion of threats poses two interrelated tasks for the study of national security strategies: first, to describe what is being securitized (and with what language/tools), and second, to explain why different states attach different “existential weight” to similar risks. It is here that a comparative approach, supported by key security theories, has practical value for analyzing and predicting trajectories of confrontation and cooperation.

In view of the outlined relevance of the research problem, the aim of the article is to identify and interpret the similarities and differences between the national security strategies of Bulgaria, the USA, Russia and China through the prism of theoretical “lenses” that consistently

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.90>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

emphasize power competition and interest (theories of realism/neorealism), institutional cooperation (theories of liberalism/neoliberalism), the role of ideas/identities (constructivism) and the processes of securitization (Copenhagen School) [6]–[10]. The practical focus is to derive stable comparative indicators (e.g. reference object, types of threats, tools, attitude towards institutions and sovereignty) that will support analytical work in a dynamically changing environment.

In connection with the formulated research objective, the subject of this study is the official framework documents for national security and a limited set of complementary documents such as white papers/texts, which serve as strategic “benchmarks” for priorities, threats and means. The core of the corpus includes: “Updated National Security Strategy of the Republic of Bulgaria” (2018) [1], US National Security Strategy (NSS, 2025) [2], “Strategy of National Security of the Russian Federation” (approved by Decree No. 400; 2021) [3], and “China’s National Security in the New Era” (May 2025) [4]. As a secondary, but methodologically useful source for the “military instrument” and the translation of strategic goals into operational feasibility, the analysis of various scholars is used, such as Milko Stefanov (2025) on operational art and the “doctrine–adaptability” dilemma [5]. The subject of the study is the comparative model of: definitions and reference objects of security; threat hierarchies (incl. cyber, information, technological and economic); instrument profiles (military and non-military means, including sanctions/protectionism, institutional mechanisms and technological policy); role of international institutions; concept of sovereignty; and mechanisms and sectors of securitization.

The author’s working hypothesis is that, on the one hand, the strategic documents of the four countries converge towards a hybrid profile, including sovereignty and “extended” security, in which topics such as cyber, technology and economic aspects are integrated into national security on a par with the classical military dimensions. On the other hand, it is observed that the strategic documents under consideration diverge along two key parameters: (1) dominant referential object (person/citizen; state; political system/regime; society/identity) and (2) attitude towards international institutions (from collective institutional embeddedness to skeptical/instrumental or competitive reading). As a sub-hypothesis, it can be assumed that where the documents securitize “multi-sector” threats and adopt multi-domain scenarios, the requirement for operational feasibility inevitably enhances the importance of organizational adaptability and the “doctrine-flexibility” synthesis, as is the argument of Stefanov (2025) [5].

II. MATERIALS AND METHODS

The study is based on an extensive corpus of official documents and analyses. At its core are the national security strategies of Bulgaria, the United States, Russia, and China. Expert analyses and reports are also used to enrich the context.

The main research methods include:

- Content analysis of strategic texts by reference object, priority threats, tools, attitude towards institutions, concept of sovereignty, securitization processes. This method allows a comparative review of the discourse and content of the strategies.
- A combined theoretical and comparative analysis by applying frameworks from realism, liberalism, constructivism and the Copenhagen School to interpret the comparable results. In this way, empirical findings are linked to academic discourses on security.

For operational purposes, the comparison is structured around five stable indicators applied uniformly across all four cases: referent object, hierarchy of threats, instruments, attitude towards institutions, and concept of sovereignty.

This study has several limitations. First, although the core comparison is anchored in official strategy documents, part of the contextual interpretation relies on secondary literature. This is especially relevant where strategic vocabulary carries strong domestic doctrinal meanings that are not always fully transferable across languages. Second, the Chinese case is examined primarily through an English-language institutional translation rather than through a systematic reading of the full original Chinese-language primary corpus. Third, while the official 2021 Russian national security strategy was consulted, the study did not systematically analyze the broader Russian-language primary corpus of complementary doctrinal, sectoral, and implementation documents in the original. The Russian and Chinese sections should therefore be read as analytically grounded but not exhaustive reconstructions of each state’s strategic discourse.

A further limitation follows from the design of the study itself. The corpus is intentionally selective and centered on framework strategies plus a limited number of complementary texts; it does not cover the full implementation layer of defence planning, budgeting, force development, or interagency practice. In addition, the analysis is qualitative and interpretive, which makes it suitable for identifying stable indicators and theoretical patterns, but less suitable for measuring policy outcomes or predicting future behavior with precision.

III. RESULTS AND DISCUSSION

A. Realism and Neorealism: Theoretical Context and Strategic Applications

a) Theoretical context

In the field of international relations, the paradigm of realism is one of the most influential and enduring theoretical lines in the analysis of state behavior in crisis conditions. For the purposes of the report, a strict distinction between the two main directions – classical realism and neorealism – is necessary, since the two directions offer different explanatory models for the origins of international rivalry and the logic of state behavior.

Classical realism emphasizes the anthropological factor and views international politics as a constant striving for dominance. Hans Morgenthau, as the founder of classical realism in the modern era, connects politics with the constant striving for power and formulates the understanding that the national interest should be thought of “in the categories of power”. In this sense, conflict and rivalry are not random deviations, but arise from the persistent tendency towards supremacy, also denoted by the concept of *animus dominandi*. According to Morgenthau, political realism is not limited to an apology for aggression, but also includes the idea of prudence as a key virtue of state action. [11, pp. 4-15].

Neorealism (structural realism), developed by Kenneth Waltz, makes a radical turn, emphasizing the systemic factor. The author argues that the behavior of states does not depend on their internal character (democracies or dictatorships), but on the anarchic structure of the international system. Since there is no “world government”, states are forced to act in a “self-help” mode, because they cannot rely on a higher guarantor for their security and survival. [12, pp. 88-99]. It is for this reason that Waltz is usually associated with the line of the so-called defensive realism (states seek balance and security, not necessarily dominance). Within the realist tradition, John Mearsheimer introduces offensive realism. According to him, the most favorable strategic outcome for a great power is not simply the accumulation of additional capabilities, but achieving a position of regional hegemony, since it is this that provides the highest degree of security in a competitive international environment. [13, pp. 16-21].

b) Strategic applications

• USA

In the NSS (November 2025) of the USA, developed by the Donald Trump administration, a hybrid concept is observed, which in the text is defined as “Principled Realism” [2, pp. 5-8], an official doctrine introduced in the 2017 strategy, but in political science it is analyzed as “Transactional Realism” [14]. Seen through the prism of realism, the concept of NSS 2025 is “Principled Realism” because the document returns to the classical principles of sovereignty and national interest, rejecting idealistic attempts to “export democracy”. In parallel, the principle of “Flexible Realism” is formulated, according to which the USA seeks good and peaceful trade relations “without imposing... democratic or other social change” on other nations [2, p. 9]. Although the term “Principled Realism” is not used as a separate concept, these provisions support the thesis that the document distances itself from ideological foreign policy goals and returns to sovereignty and interest as a legitimizing framework. The emphasis placed by the USA is on leadership and “Peace through Strength” [2, pp. 8-9], which is a direct application of Mearsheimer’s theses on the regional hegemon. Realism here is focused on the “ends-means” relationship. The referent object is the state, whose security depends on control over its borders and industrial base. In this sense, the realist reading of the NSS (2025) does not treat the economy as a separate sphere, but as the material basis of

national power, including through technological leadership and the sustainability of supply chains [2, p. 5; pp. 13-14].

Seen from another perspective – through the prism of neorealism, the NSS (November 2025) of the USA is “Transactional Realism” [14]. The document emphasizes “economic security as national security” and the protection of sovereignty in the face of global commitments [2, pp. 5-11]. The USA views the international structure as a security market, where alliances are effective only if there is “burden sharing” [14, pp. 320-322]. The goal is to maintain a unipolar position through economic protectionism as a basis for military power.

• Russian Federation

From the perspective of realism, the National Security Strategy of Russia (Strategy of National Security (Decree No. 400, 2021) puts the “protection of traditional spiritual and moral values” at the forefront. The document presents Russia as an independent and sovereign pole capable of resisting external pressure. The conflict with the West is interpreted as a clash of wills and identities [3, section II, item 7, items 20-21], where sovereignty is an absolute value that justifies the use of force [3, section II, items 34-40]. In this sense, one can speak of classical realism, in which the information space is securitized as a new domain of military action, and security is a “state of protection” of the state interest against external pressure. This can be interpreted through the prism of Stephen Walt’s theory of the balance of threats [15, pp. 17-21]. The implicit geopolitical logic that emerges from the document is that Russia officially links its security to the elimination and prevention of hotbeds of tension in Russia’s neighboring countries, which is a classical realist model for protecting the space of immediate strategic interests. Russian strategy is a classic example of protecting “spheres of influence”. The strategy itself does not define Russia as a revisionist power, but its emphasis on sovereignty, spheres of influence, and limiting external pressure lends itself to such an interpretation. Sergei Karaganov presents Russia as a state that is restoring its hard power to deter further NATO expansion and challenge the rules of the order imposed by the West after the Cold War [16]. Here, realism explains the conflict as a clash of geopolitical spaces, where “security for one is a threat to the other” (the security dilemma). If we look at Russia’s strategy through the prism of neorealism, we will notice that the Russian Federation defines the international environment as “the transformation of the world order with an increasing number of centers of power”. The text, analyzing the structural shift of layers, also points out the need for coordination between different centers of development through multilateral cooperation, and not through bloc approaches [3, section I, item 9].

• People’s Republic of China

In the context of realism, China’s National Security in the New Era (May 2025) focuses on “political security” – the survival of the regime and the leadership of the Chinese Communist Party, which are identified with the survival of the nation [4, p. 6]. In this sense, the document places

domestic political stability and regime security as the foundation of national security, which can be read in a realist perspective. Seen through the prism of neorealism, China uses in the document a logic close to the concept of “Comprehensive National Power”. The document also places a neorealist focus on the “scientific and technological revolution” as a “double-edged sword.” China defines emerging fields as key to changing the international balance of power [4, pp. 22-30]. This can be defined as structural neorealism. The document acknowledges growing strategic tensions, but at the same time rejects the thesis that the “Thucydides Trap” is a historical inevitability. The “Thucydides Trap” is a deadly pattern of structural tension that occurs when a rising power threatens to displace the ruling power and war becomes structurally likely. In his book “Destined for War,” Graham Allison explains why the “Thucydides Trap” is the best lens for understanding US-China relations in the 21st century, and through unusual historical parallels and military scenarios, he shows how close we are to the unthinkable. Yet, he emphasizes that war is not inevitable [17]. China is preparing for the inevitable structural tension with the US by changing the balance of power through innovation, not just weapons. The strategic goal is structural change of the system through technological superiority (AI, quantum technologies), avoiding direct military confrontation until the moment when the balance of power is irreversibly changed [4, pp. 18-23].

• Republic of Bulgaria

Bulgaria is in a specific situation. The Updated National Security Strategy (2018) remains the leading framework document, while the National Defense Strategy (2025) has already been adopted and reflects the new realities after 2022. This “anticipatory” updating of the sectoral strategy shows the realistic need of the military leadership to respond to threats in the Black Sea region, regardless of the delay in the political framework. In view of this, there is a need to cumulatively analyze the two documents. The Updated National Security Strategy (2018), in the context of realism, defines “vital interests” (sovereignty, territorial integrity), but still uses the language of liberal institutionalism, relying on international law as a guarantor [1, p. 18-22]. The National Defense Strategy (2025) is a much more “realistic” document than the framework. It takes into account the war in Ukraine as a direct factor and puts “national resilience” and deterrence as a priority [18, pp. 3-6]. From the perspective of neorealism, the Updated National Security Strategy (2018) recognizes the need for NATO membership, which can be perceived as the only way to survive in the anarchic environment of, for example, the Black Sea region. In terms of the National Defense Strategy (2025), neorealism can be interpreted as Bulgaria’s desire to strengthen its capabilities and alliance integration in the context of growing confrontation between Russia and NATO [18, pp. 10-12].

For the purposes of the analysis, in a deductive form it can be stated that realism is a useful tool because it explains why countries with different ideologies act in a similar way

(e.g. the USA and China fight for influence in the seas). On the other hand, it allows us to understand that the Black Sea will always be a zone of confrontation, while Russia and NATO have incompatible ideas about their security in the region. Last but not least, it shows that “strategic autonomy” is a luxury that great powers can afford, and in the context of Bulgaria, security is a function of the strength of the alliances in which it participates.

B. Liberalism and Neoliberal Institutionalism: Theoretical Context and Strategic Applications

While the realist paradigm emphasizes the inevitability of conflict in conditions of anarchy, the liberal tradition in international relations explores the mechanisms through which cooperation becomes a rational and sustainable choice for states.

a) Theoretical context

The theoretical foundation of the liberal approach to international relations is rooted in the principles of classical liberalism, the main pillar of which is the concept of individual freedom and state legitimacy arising from the consent of the governed. According to John Locke in his “Second Treatise of Government” (1689), the main role of the state apparatus is the protection of the natural rights of the individual – life, liberty and property [19]. In this context, the internal political structure of the state is seen as a decisive factor for its external legitimacy. This classical emphasis on the “internal character” of the political community lays the foundation for the understanding that states are not homogeneous actors, and their behavior on the international stage is a direct reflection of their internal structure and values.

The transition to modern liberalism is most clearly argued by Michael Doyle, who adapts Immanuel Kant’s ideas about “perpetual peace” to contemporary political reality. According to Doyle, the internal political structure of the state is a primary factor in its international behavior. The central thesis is that liberal democracies build a “zone of separate peace” among themselves. This is due to a combination of republican institutional constraints (where the will of citizens acts as a brake on war) and shared liberal norms that guarantee mutual recognition of legitimacy [20, pp. 1151, 1157-1160]. It is important to note that this peace is specific only to relations between liberal regimes, while they can show aggression towards illiberal ones.

The theory of neoliberal institutionalism adopts the neorealist assumption of an anarchic international system composed of rational egoists. According to Robert Cohen, what is characteristic is that international institutions (regimes) qualitatively change the calculations of states. Institutions reduce transaction costs, solve problems of information deficit and create a “shadow of the future” (repeatability of relations), which makes long-term cooperation more profitable than short-term unilateral aggression [21, pp. 51-65, 85-109].

The complementarity of the two theories postulates that a high degree of economic integration and the “spirit of trade” raise the cost of conflict to levels that make it an

irrational instrument of national policy. The liberal state views security not only as military survival, but also as preserving the conditions for economic prosperity.

b) Reflection in strategic documents

• USA

The new US NSS (2025) demonstrates a shift from global liberalism to instrumental neoliberalism. The document does not present international institutions as an end in itself, but as useful insofar as they support American interests, sovereignty, and burden-sharing. The US strategy defines alliances as “a broad network of alliances,” but at the same time formulates the principle of “Primacy of Nations,” according to which the nation-state remains the primary political entity, and international institutions should be evaluated according to whether they strengthen, rather than limit, national capacity for action [2, pp. 6, 9]. Arguably, we can point out that according to Trump, institutions are useful only if they serve American technological competitiveness and share the financial burden. In this sense, Trump’s NSS 2025 marks a transition to transactional neoliberalism. This logic is also confirmed in the section “Burden-Sharing and Burden-Shifting”, where it is insisted that allies take greater responsibility for security in their regions [2, p. 12]. Therefore, it is most accurate to define the strategy as an example of selective instrumental institutionalism, rather than universalist liberalism.

• Russian Federation

The 2021 National Security Strategy of the Russian Federation contains a clear criticism of the Western countries’ desire to maintain their hegemony, the weakening of international institutions, and the crisis of the Western liberal model. In this sense, the document reflects a strong skepticism towards the Western-dominated international order and the use of sanctions, political, and information pressure as tools of rivalry [3, sec. II, paras. 7, 19, 21]. At the same time, it would be inaccurate to claim that the strategy simply places sovereignty “above” international law. It is more accurate to say that it combines the protection of sovereignty with an insistence on international relations based on international law, equal and indivisible security, and the strengthening of universal international institutions. The document also speaks of multilateral interaction “without dividing lines and bloc approaches,” as well as mechanisms for coordinating the interests of different centers of development [3, sec. II, paras. 9, 24; sec. IV, paras. 97, 101]. Russia is striving to build alternative “illiberal” formats for cooperation (e.g. BRICS, Shanghai Cooperation Organization) that exclude the Western model of universal values. Therefore, a more correct qualification is institutional skepticism towards the Western-dominated order, rather than a complete rejection of the international legal and multilateral framework as such.

• People's Republic of China

The document China’s National Security in the New Era focuses on political security, a systematic approach,

and coordination between security and development. The English version used emphasizes that national security should place people’s security at the core, political security as the foundation, economic security as the cornerstone, and rely on coordinated development of security and growth [4, p. 12]. In China’s National Security in the New Era (2025), China demonstrates a complex strategy for “institutional transformation.” China maintains active participation in existing institutions (UN, WTO), multilateral formats (e.g. BRICS, Shanghai Cooperation Organization) and rules, including a rules-based multilateral trading system, while simultaneously developing its own initiatives such as the Global Security Initiative [4, pp. 31-35]. Therefore, it is more accurate to interpret the document as an example of pragmatic institutionalism, rather than as evidence of pure neoliberal universalism.

• Republic of Bulgaria

Bulgaria is closest to the liberal-institutional model. In the Updated National Security Strategy of 2018, NATO membership is defined as a “strategic choice” and “one of the main guarantors of our national security”. The same section also emphasizes the multilateral approach to ensuring peace and security [1, para. 145]. The National Defense Strategy of 2025 places a clearer emphasis on collective defense, interoperability, multinational initiatives and national resilience. It explicitly states that security in the Black Sea region is possible only with the collective efforts of NATO and the EU, that Bulgaria will adapt its armed forces to NATO plans, and that national and collective resilience are key to security [18, pp. 10-11, 17]. Furthermore, the modernization of the armed forces is tied to the requirements of interoperability and standardization [18, pp. 22, 24]. Therefore, Bulgaria should be considered as an example of union institutionalism of a small state, and not simply as a “typical liberal case” in the abstract sense.

From the analysis conducted, we can justify the conclusion that the liberal and neoliberal-institutional perspectives remain useful because they show why even in a conflict environment, states continue to invest in alliances, regimes and multilateral formats. This is most clearly seen in Bulgaria and in a more pragmatic version in China. In the US, institutions are read instrumentally, and in Russia – selectively and with a high degree of skepticism towards the Western-dominated order.

At the same time, the documents also show the limits of the liberal reading. The US NSS (2025) subordinates institutions to national interest and burden-sharing. The Russian strategy criticizes Western hegemony and the selective application of norms, and the Chinese document defends multilateralism, but through a clearly state-centric framework. The Bulgarian Defense Strategy of 2025 puts deterrence, alliance commitment and resilience at the forefront. Therefore, the more accurate conclusion is not that liberalism is “failing”, but that in contemporary strategic discourse, institutional logic is everywhere subordinated to security, sovereignty and the utility of alliances.

C. Social constructivism: identity, norms and strategic narratives

While realism and liberalism focus on material factors (military power and institutions), constructivism offers a critical look at ideal factors. The main thesis is that security is not an objectively given reality, but a social construction arising from shared perceptions, identities, and historical stratifications.

a) Theoretical context

According to Alexander Wendt, international anarchy does not automatically impose a single logic of behavior. The behavior of states depends not only on material capabilities, but also on the way in which states recognize and position themselves in relation to each other [22, p. 22; pp. 247-248]. It follows that threats are not purely material. The same capabilities can be perceived differently depending on whether the other state is thought of as an enemy, a rival, or a friend. In this sense, one can speak of the intersubjectivity of the threat, and not simply of its "subjectivity" in a psychological sense [22, pp. 247-248].

States often act not only according to their material self-interest, but also according to what is considered "right" or "normal" within their specific strategic culture. In *World of Our Making*, Nicholas Onuf writes that rules, as "guiding, but not determining, human conduct," give "social meaning." States therefore act within normatively structured understandings of permissible, right, and legitimate behavior, and not only under the pressure of interest in a narrow material sense [23, p. 22].

b) Application to strategic documents and national narratives

• USA

In NSS (2025), the constructivist element is strongly expressed through a redefinition of American identity. The document does not only list interests and means, but also frames a specific image of the American political "self". The reference object is national sovereignty and the economy. The "continued survival and safety" of the USA as an "independent, sovereign republic" is placed at the center and it is stated that the country wants to protect "its way of life" from "hostile foreign influence". In addition, the strategy emphasizes the industrial base, technological leadership and the restoration of American spiritual and cultural health. Therefore, we can say that it is talking about an identity and value framing of security [2, pp. 3-4].

• Russian Federation

The Russian strategy is an example of constructivism embedded in a state document. It introduces as strategic priorities "the protection of traditional Russian spiritual and moral values, culture and historical memory" as a vital interest for security [3, sect. III, item 25(7), 26(8)]. At the same time, section II of the document presents the West as a significant value-political "other": Western countries are described as striving to preserve their hegemony; there is talk of a crisis of the Western liberal model, of attempts to dilute traditional values, of information campaigns to form

a hostile image of Russia and of using internal socio-economic problems to split Russian society. Therefore, the constructivist conclusion that security is also framed through a value-identity opposition is justified [3, sect. II, item 7, 19-21]. In this sense, the referent object is the state/civilization, and security is socially constructed around the idea of protecting "traditional values" from Western infiltration into the information space.

• People's Republic of China

In the first section of the document China's National Security in the New Era, China is presented as a source of "certainty and stability" in a "volatile and unstable world", while the global environment is described in terms of the revival of hegemonism, power politics, zero-sum games and the risks of a "double-edged" scientific and technological revolution. Therefore, one can speak of a Chinese narrative of stability, order and development, opposed to hegemonism and coercion [4, pp. 9-10]. The document frames security as "comprehensive, systematic, and relative". The English translation used states that Chinese national security "takes people's security as its purpose, political security as its foundation, and national interests as its criterion". At the same time, the document emphasizes that China coordinates its own security with common security, rejects coercive security practices and threats, and follows a national security path with Chinese characteristics. This allows us to speak of a strong ideological and political-normative framing of security [4, pp. 7-8]. In this sense, the political system can be defined as a reference object, because security is defined as "comprehensive" and inextricably linked to regime stability and social harmony.

• Republic of Bulgaria

The updated National Security Strategy of 2018 brings the security of the citizen to the forefront and explicitly states that the "true meaning" of national security is the guarantee of human security and the protection of the freedom and dignity of the citizen. In this sense, the reference object is the person/citizen. At the same time, the strategy directs the country's resources towards "unity and prosperity in accordance with the European civilizational choice", and Bulgaria is framed as a member of the EU and NATO, which also considers its security in a collective format. Therefore, one can speak of a liberal-constructivist element [1, para 3-4, 8].

The National Defense Strategy of the Republic of Bulgaria 2025 does not contain an explicit statement that threats in the information space are directly aimed at national identity. Instead, the document emphasizes that national resilience represents the "first line of deterrence and defense" and examines the information environment through the prism of strategic communications. In this context, it emphasizes the need to counter fake news, disinformation campaigns, propaganda impacts, manipulation of public opinion and processes of erosion of trust in state institutions. Therefore, it is more correct to assume that the strategy primarily addresses impacts on public trust, social attitudes and institutional resilience, and

does not formulate national identity as a direct object of attack [18, pp. 17, 19-20].

This conclusion also corresponds to the analysis of hybrid operations presented in the study by Ralitsa Borisova, which allows for a more precise interpretation of the nature of contemporary threats. The author points out that in the preparatory phase of hybrid actions, strategic, political, economic, social and infrastructural vulnerabilities of the target state are identified and exploited, including by building networks of influence and impact on the public environment. In the subsequent phase, intensive information operations are carried out, aimed at hindering the decision-making process and weakening public and institutional resilience [24, pp. 82–83]. In this sense, the emphasis on trust, public attitudes and institutional stability, laid down in the National Defense Strategy, can be interpreted as reflecting precisely these mechanisms of impact.

Constructivism is useful here because it shows why different countries attach different existential weight to similar risks. For Bulgaria, the reference object is primarily the citizen and human security, and for Russia – state sovereignty and traditional values. For China, the reference object is political security and the overall sustainability of the system, and for the US – the sovereign republic, way of life, industrial base and technological superiority. This does not cancel out material factors, but shows that they acquire strategic meaning only when framed through identities, norms and political narratives.

D. Copenhagen School: securitization as a tool of strategic discourse

While previous paradigms sought objective or normative sources of security, the Copenhagen School viewed security not as a given, but as the result of a securitizing speech act.

a) Theoretical context

A problem becomes a security issue when it is presented as an existential threat to a certain referent object and thus legitimizes extraordinary measures beyond the usual political process; full securitization also presupposes the acceptance of this presentation by a relevant audience [10, pp. 24-26]. Critically, M. C. Williams emphasizes that the distinguishing feature of securitization is precisely the logic of exception and exceptionalism through which a given issue is taken beyond normal politics [25, pp. 514-517].

In this framework, the securitizing actor is the subject who articulates a given problem as an existential threat to a relevant audience. The referent object is the value, community, or institution whose survival is presented as threatened, and the emergency measures are those actions that gain legitimacy precisely through this rhetoric of urgency, priority, and permissible deviation from normal political procedures [10, pp. 24-27, 36-37].

b) Securitization processes in current strategies

• USA

In the US NSS (2025), the logic of securitization is most visible in the economic, technological, and industrial spheres. The document explicitly links national security to protection from hostile foreign influence, predatory trade practices, secure supply chains, reindustrialization, defense industrial base, and cutting-edge technologies, including AI [2, pp. 3, 12-14]. In the section on Asia, China is presented not as an abstract civilizational threat, but as an economic and technological competitor whose influence on supply chains must be limited through reciprocity, tariffs, reindustrialization, and protection of critical dependencies [2, pp. 19-22].

• Russian Federation

Russia's 2021 Strategy expands the register of security far beyond the purely military sphere, including information, economic, scientific and technological, public and value security [3, Sect. III, item 25-26]. In Section II, the document emphasizes the growing geopolitical instability, information campaigns to form a hostile image of Russia, attempts at internal destabilization and the need to strengthen sovereignty, and in Section IV, item 47(1), the task of preventing external interference and inspiring "color revolutions" is explicitly set [3, Sect. II, items 17-21; Sect. IV, item 47(1)].

• People's Republic of China

China's 2025 National Security White Paper frames security as comprehensive, systematic, and relative. It places people's security as the goal, political security as the foundation, and national interests as the criterion [4, pp. 6, 13-14]. In this sense, securitization encompasses not only traditional military risks, but also social stability, network security, data protection, and AI. The document speaks of building security barriers for the network, data, and AI sectors, implementing the Data Security Law, data security review, and security review system for foreign investment, as well as maintaining overall social stability in the context of deep internet and technological transformation [4, pp. 22-23, 25-29].

• Republic of Bulgaria

Bulgarian strategic documents show institutionally bound securitization rather than "reactive" securitization in the strong sense of the term. The updated 2018 National Security Strategy presents migration as a potential strategic threat, takes into account the growing migratory pressure, the activation of hybrid actions, the manipulation of public opinion and disinformation, and also highlights energy security and a secure cyberspace as important national interests [1, para. 19, 30, 33 and 166]. The 2025 National Defense Strategy builds on this framework by emphasizing national resilience as the "first line of deterrence and defense," countering fake news, disinformation campaigns, and hybrid actions, as well as the risks associated with migratory pressure, energy security, secure supply chains, and digital transformation [18, para. 18-23, 87-88, 100-105].

Against this background, Milko Stefanov's argument, productive as an analytical perspective, is that

contemporary conflicts are characterized by hybrid threats, information saturation and high technological dynamics, and the success of operational art does not stem from a choice between doctrinal consistency and unlimited adaptability, but from a synthesis between the two [5, pp. 10-11, 25-27]. Applied to the strategies under consideration, this means that the securitization of the economy, data, cyberspace, artificial intelligence, migration and information environment requires not only a new language of security, but also the adaptation of organizational, operational and resource solutions.

Therefore, the usefulness of this analytical approach is two-fold. First, it allows us to identify which topics are moving from the realm of normal politics to the realm of urgency and priority: in the American case – supply chains, reindustrialization and AI; in the Russian case – sovereignty, informational psychological impact and value protection; in the Chinese case – political security, social stability and data/AI security; in the Bulgarian case – resilience, hybrid actions, migration pressure and strategic communications.

Second, the approach shows that securitization also has resource implications. In the Bulgarian case, the document does not speak of “drastic increases above 2% of GDP”, but fixes 2.0% of GDP as the already achieved minimum necessary level and the basis for subsequent increases [18, para 125]. For this reason, the precise formulation is that the securitization discourse legitimizes priority resource provision and organizational adaptation, and not automatic extraordinary budget increases beyond what is explicitly stated in the strategy.

E. Copenhagen School: securitization as a tool of strategic discourse

The comparative findings can be synthesized through the stable indicators announced in the introduction and applied throughout the analysis. Table I summarizes the country-specific observations in a common analytical matrix and makes visible the main lines of convergence and divergence between the four national security strategies.

TABLE I COMPARATIVE SYNTHESIS OF STABLE INDICATORS ACROSS THE FOUR NATIONAL SECURITY STRATEGIES

Stable indicator	Republic of Bulgaria	United States	Russian Federation	People's Republic of China
Referent object	Citizen/human security, national resilience, and alliance-embedded state security	Sovereign state, territorial control, industrial base, and the American way of life	Sovereign statehood, strategic autonomy, regime stability, and protection of traditional values	Political security, CCP leadership, system stability, people's security, and national interests
Hierarchy of threats	Black Sea instability, hybrid actions, disinformation, migration pressure, cyber and	Strategic competition with China, Russia as a major challenger, border insecurity, supply-	NATO/Western pressure, external interference, information warfare, sanctions, internal destabilization	External containment, political instability, cyber/data/AI risks, technological dependence, threats to

Stable indicator	Republic of Bulgaria	United States	Russian Federation	People's Republic of China
	energy risks	chain dependence, technological vulnerability	n, erosion of values	social stability
Main instruments	Collective defence, interoperability, modernization, strategic communications, resilience-building within NATO and the EU	Military superiority, border control, reindustrialization, tariffs and trade policy, technological leadership, selective alliances	Military deterrence, sovereign control of the information space, strategic autonomy, partnerships beyond the West, value protection	Comprehensive security governance, technological innovation, party-state control, data and cyber regulation, multilateral initiatives
Attitude towards institutions	Strong positive embeddedness in NATO and the EU; institutions as security multipliers	Selective and instrumental; institutions are useful insofar as they support U.S. interests and burden-sharing	Skeptical towards Western-led institutions; preference for alternative or plural centers of coordination	Pragmatic institutionalism; works within existing institutions while simultaneously developing parallel initiatives
Concept of sovereignty	Sovereignty protected through law, alliances, and collective defence	Primacy of the nation, autonomy of action, and control of borders and the economic base	Absolute and non-negotiable sovereignty as a shield against external interference	Sovereignty and non-interference linked to regime security, development, and political order

Source: compiled by the author on the basis of [1]–[4], [18].

As Table I shows, convergence is strongest in the expansion of security agendas beyond the strictly military domain and in the multidomain character of contemporary strategic instruments. Divergence is strongest in the dominant referent object, in the meaning attached to sovereignty, and in the role attributed to international institutions. In this sense, the comparison supports the working hypothesis only partially: the four strategies converge in what they increasingly securitize, but diverge in what they ultimately seek to protect and in the political logic through which security is organized.

IV. CONCLUSIONS AND SUMMARY

The comparative analysis shows that the four strategies share an expanded understanding of national security in which cyber, information, technological, economic, and societal dimensions are integrated with classical military concerns. This confirms the first part of the working hypothesis: in all four cases, security discourse has moved toward a hybrid and multidomain profile.

At the same time, the cases diverge in the dominant referent object, the hierarchy of threats, the role assigned to institutions, and the meaning of sovereignty. Bulgaria places citizen security, resilience, and alliance embeddedness at the centre; the United States prioritizes sovereign state capacity and industrial-technological power; Russia foregrounds sovereign statehood, strategic autonomy, and protection from external pressure; China centers political security, regime stability, and comprehensive security governance. The hypothesis is therefore only partially confirmed: convergence is strongest in the expansion of the security agenda, while divergence is strongest in the political logic of protection.

The theoretical comparison indicates that no single approach is sufficient on its own. Realism and neorealism best explain strategic rivalry, balance-of-power behavior, and the salience of military and material capabilities. Liberal and neoliberal institutionalism remain indispensable for explaining alliance dependence and the continued utility of multilateral frameworks. Constructivism and the Copenhagen School clarify how similar risks acquire different existential meanings and how new domains are securitized through strategic discourse. For Bulgaria, the main implication is that resilience, interoperability, and societal cohesion are more realistic sources of security than any strong version of strategic autonomy.

REFERENCES

- [1] National Assembly of the Republic of Bulgaria, "Updated National Security Strategy of the Republic of Bulgaria" ("Актуализирана стратегия за национална сигурност на Република България"), adopted by National Assembly decision of Mar. 14, 2018; promulgated in State Gazette, No. 26, Mar. 23, 2018, 2018 [In Bulgarian]. [Online]. Available: https://www.mod.bg/doc/strategicheski/20180330_AktualiziranaSNSRB_2018.pdf. [Accessed: Mar. 29, 2026].
- [2] The White House, "National Security Strategy of the United States of America," Nov. 2025. [Online]. Available: <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>. [Accessed: Mar. 29, 2026].
- [3] President of the Russian Federation, Presidential Decree No. 400 of July 2, 2021, "On the National Security Strategy of the Russian Federation" ("О Стратегии национальной безопасности Российской Федерации"), 2021. [Online]. Available: <http://www.kremlin.ru/acts/bank/47046/page/3>. [Accessed: Mar. 29, 2026].
- [4] China Aerospace Studies Institute (CASI), "ITOW: China's National Security in the New Era (2025)" (translation of the PRC State Council Information Office white paper, May 2025), Sept. 8, 2025. [Online]. Available: <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2025-09-08%202025%20China%20National%20Security%20White%20Paper%202025.pdf?ver=nA5qS3sBOYidpEoW77qhfw%3D%3D>. [Accessed: Mar. 29, 2026].
- [5] M. Stefanov, "Operational Art in the 21st Century – the Dilemma Between Doctrinal Consistency and Adaptive Necessity" ("Оперативното изкуство в XXI век – дилемата между доктриналната последователност и адаптивната необходимост"), *Sigurnost i Otrana* (Security and Defence) ("Сигурност и отбрана"), no. 2, pp. 9-30, 2025, <https://doi.org/10.70265/BBDU1894>.
- [6] W. J. Korab-Karpowicz, "Political Realism in International Relations," *The Stanford Encyclopedia of Philosophy*, first published 2010; substantive revision Oct. 9, 2023. [Online]. Available: <https://plato.stanford.edu/entries/realism-intl-relations/>. [Accessed: Mar. 29, 2026].
- [7] R. O. Keohane, "International Institutions: Two Approaches," *International Studies Quarterly*, vol. 32, no. 4, pp. 379–396, Dec. 1988, <https://doi.org/10.2307/2600589>. [Online]. Available: <https://www.rochelleterman.com/ir/sites/default/files/keohane1988.pdf>. [Accessed: Mar. 29, 2026].
- [8] A. Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization*, vol. 46, no. 2, pp. 391–425, 1992, <https://doi.org/10.1017/S0020818300027764>. [Online]. Available: [https://pmachala.people.amherst.edu/Current%20Politics/PS-50%20IR%20&%20Foreign%20Policy%20Theory-THE%20READINGS/Archive/Wendt,%20Anarchy%20is%20what%20states%20make%20of%20it%20\(1992\).pdf](https://pmachala.people.amherst.edu/Current%20Politics/PS-50%20IR%20&%20Foreign%20Policy%20Theory-THE%20READINGS/Archive/Wendt,%20Anarchy%20is%20what%20states%20make%20of%20it%20(1992).pdf). [Accessed: Mar. 29, 2026].
- [9] O. Wæver, "Securitization and Desecuritization," in *On Security*, R. D. Lipschutz, Ed. New York, NY, USA: Columbia University Press, 1995, pp. 46–87. [Online]. Available: <https://www.scribd.com/document/258746092/O-Waever-Securitization-and-Desecuritization>. [Accessed: Mar. 29, 2026].
- [10] B. Buzan, O. Wæver, and J. de Wilde, *Security: A New Framework for Analysis*. Boulder, CO, USA: Lynne Rienner Publishers, 1998. [Online]. Available: https://books.google.bg/books?id=j4BGr-ElsP8C&pg=PP7&hl=bg&source=gbs_selected_pages&cad=l#v=onepage&q&f=false. [Accessed: Mar. 29, 2026].
- [11] H. J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 1st ed. New York: Knopf, 1948. [Online]. Available: <https://archive.org/details/in.ernet.dli.2015.74487>. [Accessed: Mar. 29, 2026].
- [12] K. N. Waltz, *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979. [Online]. Available: https://books.google.com/books/about/Theory_of_International_Politics.html?id=OaMFAAAQBAJ. [Accessed: Mar. 29, 2026].
- [13] J. J. Mearsheimer, *The Tragedy of Great Power Politics*. New York: W.W. Norton & Company, 2001. [Online]. Available: <https://www.slideshare.net/slideshow/the-tragedy-of-great-power-politics-1pdf/266699506#30>. [Accessed: Mar. 29, 2026].
- [14] L. Bălănuță, "Transactional Realism – recasting power as bargain. The diplomatic strategy of the United States in relation with the Russia-Ukraine war," *Revista de Științe Politice. Revue des Sciences Politiques*, no. 87, pp. 319–331, 2025. [Online]. Available: https://cis01.ucv.ro/revistadestiintepolitice/files/numarul87_2025/25.pdf. [Accessed: Apr. 03, 2026].
- [15] S. M. Walt, *The Origins of Alliances*. Ithaca, NY: Cornell University Press, 1987. [Online]. Available: https://api.pageplace.de/preview/DT0400.9780801469992_A29967168/preview-9780801469992_A29967168.pdf. [Accessed: Apr. 03, 2026].
- [16] S. A. Karaganov, "Mutual Assured Deterrence," *Russia in Global Affairs*, Feb. 22, 2017. [Online]. Available: <https://eng.globalaffairs.ru/articles/mutual-assured-deterrence/>. [Accessed: Apr. 03, 2026].
- [17] G. Allison, *Destined for War: Can America and China Escape Thucydides's Trap?*. Boston: Houghton Mifflin Harcourt, 2017. [Online]. Available: <https://www.hks.harvard.edu/publications/destined-war-can-america-and-china-escape-thucydides-trap>. [Accessed: Apr. 03, 2026].
- [18] Ministry of Defence of the Republic of Bulgaria, "National Defence Strategy of the Republic of Bulgaria" ("Национална отбранителна стратегия"), adopted by Council of Ministers Decision No. 131 of Mar. 6, 2025 [In Bulgarian]. Sofia, Bulgaria, 2025. [Online]. Available: https://www.mod.bg/doc/strategicheski/20250324_Natsioanalna_otbranitelna_strategia_RMS_131_06.03.2025.pdf. [Accessed: Apr. 3, 2026].
- [19] J. Locke, "Two Treatises of Government" ("Dva traktata za upravlението" / "Два трактата за управлението"), S. Malinov,

- Trans. Sofia, Bulgaria: Iztok-Zapad, 2022, ISBN: 978-619-01-1000-2. [In Bulgarian].
- [20] M. W. Doyle, *Liberalism and World Politics*, American Political Science Review, vol. 80, no. 4, pp. 1151-1169, 1986. [Online]. Available: <https://rochelleterman.com/ir/sites/default/files/doyle%201986.pdf>. [Accessed: Apr. 04, 2026].
- [21] R. O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press, 1984. [Online]. Available: <https://professor.pucgoias.edu.br/sitedocente/admin/arquivosUpload/17973/material/KEOHANE%20After%20Hegemony%20-%20Cooperation%20and%20Regimes.pdf>. [Accessed: Apr. 04, 2026].
- [22] A. Wendt, *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999. [Online]. Available: <https://www.guillaumenicaise.com/wp-content/uploads/2013/10/Wendt-Social-Theory-of-International-Politics.pdf>. [Accessed: Apr. 05, 2026].
- [23] N. Onuf, *World of Our Making: Rules and Rule in Social Theory and International Relations*. Columbia: University of South Carolina Press, 1989. [Online]. Available: <https://www.scribd.com/document/1004478733/Ebook-World-of-Our-Making-Rules-and-Rule-in-Social-Theory-and-International-Relations-by-Nicholas-Greenwood-Onuf-ISBN-9780415630399-0415630398-ava>. [Accessed: Apr. 05, 2026].
- [24] R. Borisova, "Hybrid operations as a tool of contemporary strategic confrontation" ("Хибридни операции като инструмент на съвременната стратегическа конфронтация"), *Sigurnost i Otrana* (Security and Defence) ("Сигурност и отбрана"), no. 2, pp. 74–89, Dec. 2025, doi: 10.70265/BSCM4111. [Online]. Available: <https://doi.org/10.70265/BSCM4111>. [Accessed: Apr. 05, 2026].
- [25] M. C. Williams, „Words, Images, Enemies: Securitization and International Politics“, *International Studies Quarterly*, vol. 47, no. 4, pp. 511-531, 2003. [Online]. Available: <https://ir101.co.uk/wp-content/uploads/2017/11/williams-words-images-enemies.pdf>. [Accessed: Apr. 07, 2026].

Radiogenic Heat Production in the Earth's Crust of Bulgaria: The Dominant Role of the Rhodope Massif

Yanitsa Boyanova

"Vasil Levski" National Military University
Veliko Turnovo, Bulgaria
yanicab89@gmail.com

Abstract— This report evaluates the radiogenic heat production (A) within the continental crust of Bulgaria, emphasizing the dominant role of the Rhodope Massif. The generation of thermal energy through the radioactive decay of uranium (U), thorium (Th), and potassium (K) is a primary component of the Earth's heat flow.

The analysis first establishes a baseline for Bulgaria by assessing the average heat production levels across the main lithological units, utilizing previously published data on their radioactive element content. Subsequently, the study focuses on the Rhodope Massif, identified as the country's most significant heat-generating region due to radiogenic values that substantially exceed the national average.

Comparative results indicate that this elevated radiogenic heat is a major driver of regional geothermal activity and the high density of thermal springs. These findings provide essential data for crustal thermal modeling and the assessment of deep geothermal energy potential in Southern Bulgaria.

Keywords - Radiogenic heat production; Rhodope Massif; geothermal energy; radioactive decay; continental crust; energy independence.

I. INTRODUCTION

The increasing global demand for sustainable and carbon-neutral energy sources has revitalized scientific interest in the Earth's internal thermal regime. Aside from the Earth's primordial heat content remaining from its formation stages, the most significant internal heat source is the continuous radioactive decay of unstable isotopes of uranium (^{238}U and ^{235}U), thorium (^{232}Th), and potassium (^{40}K). These isotopes are non-uniformly distributed within the Earth's layers, with a primary concentration in the continental crust and upper mantle. The heat generated by their decay contributes decisively to the planet's overall thermal flux, governing tectonic processes and the

formation of geothermal reservoirs. The mean surface heat flow of the Earth amounts to approximately 65 mW.m^{-2} [1], while the mantle heat flow in continental regions is estimated at roughly 28 mW.m^{-2} [2]. The significant discrepancy between these two values is attributed to the active production of heat through radiogenic processes within the continental crust itself. This crustal contribution often accounts for 40% to 60% of the total observed surface heat flow, depending on the lithological composition and tectonic history of the region [14]. The two primary isotopes of uranium, ^{238}U and ^{235}U , decay into stable lead isotopes— ^{206}Pb and ^{207}Pb respectively—with half-lives of 4.5 and 0.71 billion years. Uranium is defined as a widespread and highly mobile trace element within the composition of many rock types, particularly felsic igneous rocks. On the other hand, thorium (^{232}Th), with a half-life of 14.1 billion years, also decays into lead ^{208}Pb . Unlike uranium, thorium is chemically relatively inert and often exhibits a strong affinity for clay minerals and heavy accessory minerals. The sole unstable isotope of potassium is ^{40}K , which occurs in many rock-forming and clay minerals in significant concentrations of several percent, providing a constant and predictable component to the total radiogenic heat production. In the context of Bulgaria, the spatial distribution of these elements is controlled by the complex tectonic boundary between the stable Moesian Platform and the Alpine orogenic belt. Understanding this distribution is not only a matter of geophysical modeling but a prerequisite for assessing the country's sovereign energy potential. This report aims to evaluate the radiogenic heat production across Bulgaria's diverse geological domains, with a specific focus on the Rhodope Massif as a primary driver of the national thermal balance.

II. PHYSICAL AND GEOCHEMICAL FOUNDATIONS OF RADIOGENIC HEAT PRODUCTION

Radioactive decay fundamentally transforms mass into energy. In the initial stage, this energy is released as kinetic

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.144>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

energy of the participating particles and nuclei (alpha and beta particles, and recoiling nuclei), subsequently transforming into gamma-ray and X-ray energy, as well as geo-neutrinos. With the exception of the negligible amount carried away by geo-neutrinos, all of this energy is converted into heat in the immediate vicinity of the decaying nucleus. The volumetric radiogenic heat production of a given rock, A (measured in $\mu\text{W}\cdot\text{m}^{-3}$), is calculated using the Rybach equation [3]:

$$A = 10^{-5} \rho (9.52c_U + 2.56c_{Th} + 3.48c_K) \quad (1)$$

Where ρ represents the rock density ($\text{kg}\cdot\text{m}^{-3}$) and c_U , c_{Th} , and c_K are the respective concentrations of uranium, thorium (in ppm), and potassium (in %). The quantities of these elements vary significantly depending on the rock type but follow distinct patterns due to their similar geochemical behavior during magmatic differentiation, sedimentation, and metamorphism.

- Igneous Rocks

During magmatic differentiation, U and Th, and to some extent K, tend to enrich within the more acidic (felsic) phases. The correlated behavior of uranium and thorium is driven by their similar ionic radii and high valency. Although absolute concentrations vary relative to the degree of differentiation, the average Th/U and K/U ratios remain relatively constant. According to established models [3] [4], the contribution to total heat production in igneous rocks is distributed as approximately 40% for U, 45% for Th, and 15% for K. It is precisely this enrichment in felsic phases that makes the granitoids of the Rhodope Massif a primary subject of interest for this study.

- Sedimentary Rocks

In sedimentary environments, uranium and thorium alter their behavior because uranium is easily oxidized ($\text{U}^{4+} \rightarrow \text{U}^{6+}$), becoming highly mobile in solution. Consequently, the Th/U ratio shows significant variations reflecting pH and redox conditions. The lowest radiogenic heat production values are observed in carbonate rocks (limestones and dolomites) and evaporites. Conversely, argillaceous sediments and shales are characterized by the highest values due to the high adsorption of radioactive elements onto fine-grained materials. Sandstones and conglomerates exhibit intermediate values, which are strongly dependent on the provenance of the detrital material and the geochemical conditions prevalent during sedimentation.

- Metamorphic Rocks

Metamorphic rocks inherit the radioactive composition of their protoliths (igneous or sedimentary), but the U, Th, and K content is redistributed according to the metamorphic grade. Generally, there is a trend of decreasing concentrations of these elements as the metamorphic grade increases, driven by dehydration and the partial migration of fluids. The depletion of U and Th caused by progressive metamorphism is particularly

pronounced in granulite facies. The ions U^{4+} and Th^{4+} , characterized by large ionic radii, can exist only in eightfold coordination with oxygen and cannot be accommodated within the tightly packed structures formed under higher pressures and temperatures. Consequently, U and Th tend to migrate upward within the Earth's crust as a result of dehydration reactions or partial melting near the base of the crust [3]. Metamorphic mineral transformations lead to the loss of volatiles, with the migration of U and Th being accompanied by H_2O and/or CO_2 . Potassium appears to be relatively stable and is not significantly affected by these processes.

III. REGIONAL ANALYSIS AND QUANTITATIVE MODEL OF RADIOGENIC HEAT PRODUCTION IN BULGARIA

The territory of Bulgaria is characterized by a complex geological structure resulting in significant variations in the thermal field.

The primary division is defined by the boundary between the stable Moesian Platform to the north and the tectonically active structures of the Alpine Orogen to the south. While the north remains energy-passive due to its thick sedimentary cover of limestones and dolomites, the southern regions function as a massive crustal heat source. This is attributed to the exposed crystalline basement, enriched with Paleozoic and Tertiary granitoids, which generate intense autochthonous heat.

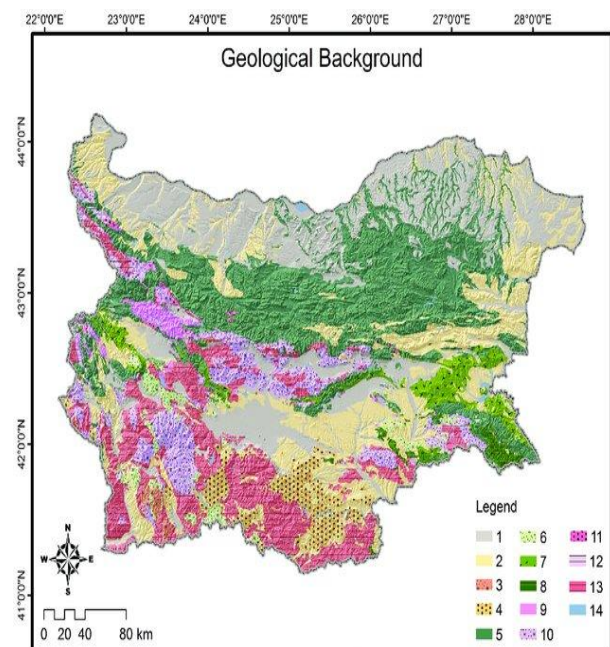


Fig 1: Geological map of Bulgaria showing the main types of rocks (after Cheshitev and Kanchev, 1989). Legend: 1 -Quaternary sediments; 2 -Neozoic sedimentary rocks; 3 -Neozoic intrusive rocks; 4 -Neozoic volcanic and volcano-sedimentary rocks; 5 -Mesozoic sedimentary rocks; 6 -Mesozoic intrusive rocks; 7 -Mesozoic volcanic and volcano-sedimentary rocks; 8 -Mesozoic metamorphic rocks; 9 -Paleozoic sedimentary rocks; 10 -Paleozoic intrusive rocks; 11 -Paleozoic volcanic

and volcanosedimentary rocks; 12 -Paleozoic metamorphic rocks; 13 -
 Precambrian metamorphic rocks; 14 -water.[5],[6]

To precisely determine the total energy capacity (Q_{total}) of the country, a computational model has been applied that categorizes these regions into three specialized lithological domains. The total heat generation for the 111,000 km² territory is calculated using the equation:

$$Q_{total} = \sum(A_i \cdot S_i \cdot D_i) \quad (2)$$

Where A_i is the radiogenic production, S_i is the occupied area, and D_i is the thickness of the active layer in the upper crust (fixed at 10 km). In this model, Bulgaria's area is weighted according to three primary types of geological environments:

- Sedimentary Basins (around 55% of the area):

Comprising the Moesian Platform and the Thracian Depression. Dominated by Mesozoic and Cenozoic sediments, primarily limestones, dolomites, marls, sandstones, and evaporites. These are typically characterized by low radiogenic isotope concentrations..

- Folded Mountain Ranges (around 25% of the area):

Including the Balkan Mountains (Stara Planina) and the Srednogorie zone. They represent a transition zone with a mixed composition of Paleozoic and Mesozoic sediments and volcanics. Includes flysch, argillites, andesites, and tuffs (common in the Srednogorie zone), along with low-grade metamorphics such as phyllites and chlorite schists.

- Crystalline Massifs (around 20% of the area):

Covering the Rhodopes, Rila, Pirin, and Sakar. This is the country's energy core, with a high-grade metamorphic and igneous complexes. Primarily composed of gneisses, migmatites, and amphibolites, along with massive intrusions of granites, granodiorites, and syenites. These lithologies host the highest concentrations of U, Th, and K.

The volumetric radiogenic heat production rate (A) for each lithological domain was derived as a weighted average based on previously published geochemical and petrophysical datasets of radionuclide concentrations in Bulgaria [11]. The spatial distribution and surface area (S_i) of the respective domains were calculated via 1:500,000 Geological Map of Bulgaria. The thickness of the radiogenic active layer (D_i) was fixed at a conservative baseline of 10 km, corresponding to the average depth of the upper brittle continental crust where granitoids and metamorphic rocks are predominantly concentrated. The total power (Q_{total}) was mathematically integrated by aggregating the discrete thermal contributions of each lithological zone, ensuring a scalable numerical model for regional geothermal forecasting.

The physical parameters and power distribution are presented in Table 1.

TABLE 1 RADIOGENIC HEAT PRODUCTION IN BULGARIA

Domain (Map Groups)	Area (S) in km ²	Density (ρ) in kg/m ³	Produc tion (A) in μ W/m ³	Calculat ed Power (P)
Sedimentary Basins	61000 (55%)	2450	1.00	~ 610 GW
Mountain Ranges	27700 (25%)	2600	1.50	~ 415 GW
Crystalline Massifs	22300 (20%)	2700	2.80	~ 624 GW
Total (Bulgaria)	111 000	—	—	1649 GW

The calculations indicate that the total radiogenic heat power in the upper crust of Bulgaria amounts to approximately 1649 GW. The average radiogenic generation per unit area is 14.8 mW/m², representing nearly 40% of the total continental heat flow.

To understand the actual significance of different geological structures for Bulgaria's energy balance, it is necessary to compare the surface area they occupy with the thermal power they actually generate.

In Sedimentary Basins, which cover more than half of the country's territory (55%), a significant deficit in heat production is observed—they contribute only 37% of the total radiogenic power. This contrast confirms that the massive accumulations of limestones and dolomites in Northern Bulgaria are energy-passive.

At the same time, the situation for Crystalline Massifs (Rhodopes, Rila, Pirin, and Sakar) is fundamentally different. Although they occupy only 20% of Bulgaria's land area, their contribution to the total power is nearly 38% (624 GW). This means that a unit area of the crystalline basement in Southern Bulgaria generates nearly twice as much energy compared to sedimentary regions.

This visual contrast clearly demonstrates that the Rhodope region and the crystalline massifs function as the country's "energy core."

The presented chart illustrates a key correlation: geographic distribution does not correspond to energy capacity.

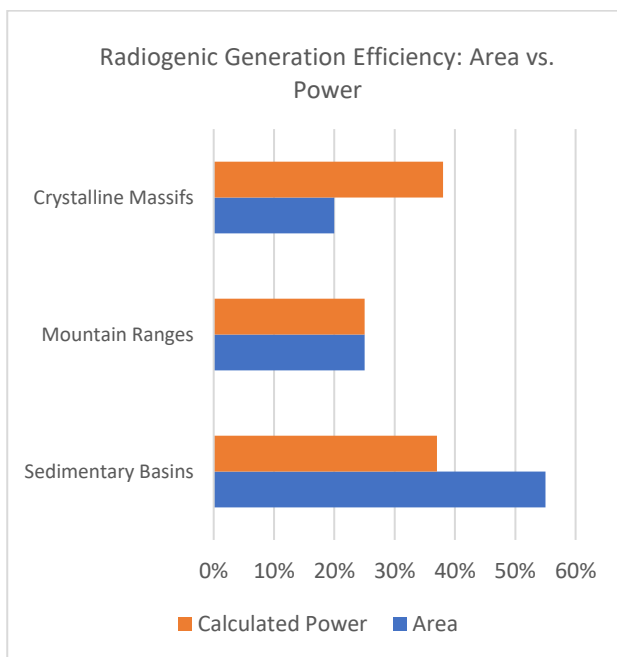


Fig 2 Radiogenic Generation Efficiency: Area vs. Power

IV. THE DOMINANT ROLE OF THE RHODOPE MASSIF

The analysis of radiogenic radiation in Bulgaria unequivocally defines the Rhodope Massif as a fundamental energy pillar in the country's architecture. Its dominant role is not a random statistical anomaly but a direct consequence of the complex geological evolution of the Balkanides, which has transformed the region into a unique thermal generator. While the majority of the country's territory is covered by Paleozoic and Cenozoic energy-passive sediments, the Rhodope Massif exposes the ancient crystalline basement of the continental crust. Composed of high-grade metamorphic rocks such as gneisses and migmatites, intruded by massive Paleozoic granitoids, this basement functions as a natural accumulator of heavy radioactive isotopes [8]. In these structures, the concentration of radiogenic elements is many times higher than in the Moesian Platform, turning the massif into a constant source of energy generated at depth [9].

This internal power is complemented by the region's specific fault tectonics, characterized by deep structural disturbances. These are of critical importance to the thermal regime, as they allow groundwater to circulate at significant depths where it absorbs heat from energy generated by radioactive decay, returning to the surface as active hydrothermal systems [6]. It is precisely the presence of this crystalline heat source that causes the uniquely high temperature gradient of the mineral springs in Southern Bulgaria, making them a direct manifestation of the endogenous energy of the subsurface.

Beyond statistical data, the geothermal potential of the Rhodope Massif assumes a strategic dimension that exceeds the scope of conventional thermal water utilization. The high density of heat production defines the region as the only zone in Bulgaria suitable for implementing innovative systems for extracting energy from hot dry rocks. The centralized nature of conventional energy sources renders them vulnerable to hybrid threats or physical damage to transmission infrastructure. On the other hand, the geothermal capacity of Southern Bulgaria allows for the establishment of a decentralized network of energy hubs located directly above zones of peak radiogenic activity. Such a distributed energy architecture enhances the resilience of the national economy during emergencies, ensuring an uninterrupted power supply for critical infrastructure [7]. Thus, the massif can be positioned as a primary factor in the national strategy for energy independence, offering a resource for the production of clean baseload electricity that is entirely independent of climatic conditions and fluctuating renewable sources.

V. CONCLUSIONS

The conducted research on radiogenic heat production in Bulgaria confirms that the country possesses a significant and largely untapped energy asset within its crystalline basement. The integrated analysis of geological, geophysical, and energy data reveals a profound regional asymmetry between the energy-passive sediments of Northern Bulgaria and the highly productive thermal core of the Rhodope Massif.

In practical terms, the quantitative model developed in this study serves as a foundational baseline for macro-level geothermal zoning and regional energy planning in Southern Bulgaria [13]. Specifically, these findings can be directly applied by resource developers and policymakers to identify optimal geographic locations for Enhanced Geothermal Systems and Deep Hot Dry Rock exploration [12]. Furthermore, incorporating this radiogenic heat data into national energy security frameworks will facilitate the strategic deployment of decentralized, climate-independent baseload power hubs, directly accelerating Bulgaria's transition toward sustainable energy sovereignty.

REFERENCES

- [1] G. R. Beardsmore and J. P. Cull, *Crustal Heat Flow: A Guide to Measurement and Modelling*. Cambridge, UK: Cambridge Univ. Press, 2001.
- [2] H. N. Pollack, S. J. Hurter, and J. R. Johnson, "The new global heat flow compilation," Dept. Geol. Sci., Univ. Michigan, Ann Arbor, MI, USA, Tech. Rep., 1990.
- [3] L. Rybach, "Determination of heat production rate," in *Handbook of Terrestrial Heat-Flow Density Determination*, R. Haenel, L. Rybach, and L. Stegena, Eds. Dordrecht, Netherlands: Kluwer Academic Publishers, 1988, pp. 311–349.

- [4] C. Jaupart and J. C. Mareschal, "The thermal structure and evolution of the continental crust," in *Treatise on Geochemistry*, vol. 3, R. L. Rudnick, Ed. Oxford, UK: Elsevier-Pergamon, 2003, pp. 65–123. :
- [5] G. Cheshitev and I. Kanchev, *Geological Map of the Republic of Bulgaria at 1:500,000 Scale*. Sofia, Bulgaria: Ministry of Environment and Waters, 1989.
- [6] T. Vasileva, "An assessment of potential groundwater recharge zones in Bulgaria," *Geologica Balcanica*, vol. 48, no. 1, pp. 43–61, Nov. 2020. doi: <https://doi.org/10.52321/GeolBalc.48.1.43>
- [7] S. Velev, "Geothermal resources of Bulgaria: Status and prospects," in *Proc. World Geothermal Congress 2005*, Antalya, Turkey, 2005, pp. 1–7. [Online]. Available: <https://www.geothermal-energy.org/pdf/IGAstandard/WGC/2005/0134.pdf>
- [8] I. Gerdjikov and N. Georgiev, "The crystalline basement of the Rhodope Massif: Tectonic and metamorphic evolution," *J. Bulg. Geol. Soc.*, vol. 72, no. 1-3, pp. 115–140, 2011.
- [9] D. Hasterok and D. S. Chapman, "Heat production and thermal state of the continental lithosphere," *J. Geophys. Res. Solid Earth*, vol. 12, no. 10, pp. 1–19, Oct. 2011.
- [10] V. Čermák, "Results of heat flow studies in Czechoslovakia and neighboring countries," in *Terrestrial Heat Flow and the Lithosphere Structure*, V. Čermák and L. Rybach, Eds. Berlin, Germany: Springer-Verlag, 1994, pp. 27–40.
- [11] D. Hasterok, M. Gard, and J. Webb, "On the radiogenic heat production of metamorphic, igneous, and sedimentary rocks," *Geoscience Frontiers*, vol. 9, no. 6, pp. 1777–1794, Nov. 2018. doi: <https://doi.org/10.1016/j.gsf.2017.10.012>
- [12] D. Brown, L. Duchane, G. Heiken, and V. T. Henri, *Mining the Earth's Heat: Hot Dry Rock Geothermal Energy*. Berlin, Germany: Springer, 2012.
- [13] K. Bojadgieva, "General overview of geothermal energy in Bulgaria," *Acta Montanistica Slovaca*, vol. 12, no. 1, pp. 58–63, Jan. 2007.
- [14] C. Jaupart and J. C. Mareschal, "Heat flow and thermal structure of the lithosphere," in *Treatise on Geophysics*, Vol. 6: Crust and Lithosphere Dynamics, G. Schubert, Ed. Amsterdam, Netherlands: Elsevier, 2007, pp. 217–251.

Environmental, Sanitary and Health Requirements in the Design and Operation of Radiation-Hazardous Facilities

Stefko Burdzhiev

*Department of Security and Safety
Varna Free University "Chernorizets Hrabar"
Varna, Bulgaria
stefko.burdzhiev@vfu.bg*

Georgi Georgiev

*Department of Security and Safety
Varna Free University "Chernorizets Hrabar"
Varna, Bulgaria
georgi.georgiev@vfu.bg*

Abstract— The article examines environmental, sanitary and health requirements in the design, development and operation of radiation-hazardous facilities, as well as the protection of personnel, the population and the environment. It discusses the main sources of radiation hazard, the principles of justification, optimization and dose limitation, engineering barriers, zoning, radiation monitoring, individual dosimetric control, personal and collective protective equipment, decontamination and the role of emergency planning. Emphasis is placed on the preventive approach: safety must be embedded at the design stage and maintained during operation through technological discipline, continuous control, training and clear coordination between the licensee, the regulatory authorities and the forces of the Unified Rescue System. Practical recommendations are proposed to increase preparedness for radiation accidents and improve real-time data exchange.

Keywords—radiation pollution; radiation-hazardous facility; radiation safety; protection design; safety design.

I. INTRODUCTION

Modern industrial production concentrates large amounts of energy, hazardous substances and complex technological processes. This turns some industrial facilities into a constant source of technogenic risk, which in the event of an unfavourable combination of technical failure, human error, natural impact or malicious action can lead to an accident with consequences for people and the environment. Radiation hazardous facilities occupy a special place in this system, because the potential impacts are not limited to the facility site, but can affect settlements, agricultural areas, water resources and critical infrastructure [1, 2].

A radiation-hazardous facility (RHF) is an object or facility where, under conditions of normal operation, accident or destruction of the facility, exposure of

personnel and the population, as well as/or radioactive contamination in the area of the facility or outside it above the natural gamma background, may occur. This group includes nuclear facilities and facilities with sources of ionizing radiation, repositories for radioactive sources and radioactive waste, laboratories, specialized medical institutions, industrial and scientific structures, as well as activities in which radioactive materials are generated, stored or transported [3, 4].

The main feature of radiation risk is that radiation safety cannot be guaranteed only by reacting after an incident. Prevention and management of radiation risk must be embedded in the entire life cycle of the facility from design to cessation of activity and scrapping: selection of the appropriate site, design fully compliant with the Act on the Safe Use of Nuclear Energy (ASUNE), construction, commissioning, normal operation, repair, emergency preparedness, decommissioning and waste management [3]. Therefore, radiation safety should be considered as an integrated system of regulatory, engineering, technical, organizational, medical, communication, etc. measures [5–7].

The goal of the report, is to examine the potential radiation risk, its relationship with natural and man-made disasters, as possible causes of radiation pollution, the prevention and management of radiation risks, the accumulation of deeper knowledge about the connectivity and interdependence of individual radiation hazardous sites (RHS) and their elements, showing possible connections and models of protection of their personnel, the population and the environment, based on national and international experience, that of the European Union (EU) and North Atlantic Treaty Organization (NATO) member states.

Based on the above, the hypothesis has been built for the establishment and definition of the protection of the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.115>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

personnel of the RHS, the population and the environment in the event of radiation contamination, as a systematic and organized activity, and the effectiveness of the protection - as a result of the actions of the many specialized interested organizations (institutions), united in a system of systems - the unified rescue system (URS); national security protection system (NSPS), etc., and this is already at the stage of their design.

The thesis being defended is that the prevention and management of the risk of radiation contamination is a systemic activity and its continuity (sustainability) is most effectively guaranteed by protection built as a system, a subsystem of the national security system of the state.

The object of study are the requirements for ensuring the security and continuity (sustainability) of the activities of radiation hazardous facilities and the continuity (sustainability) of the operation of the national system for monitoring and management of radiation risk.

The subject of the study is the environmental, sanitary and health requirements in the design and operation of a RHF, as well as some aspects of the interconnection and organization of activities, interaction and coordination of competent national authorities and organizations for monitoring and management of the risk of radiation pollution, in natural and man-made disasters, in order to ultimately guarantee their safety and sustainable operability.

II. MATERIALS AND METHODS

A. *Radiation safety and protection in the design of radiation hazardous sites (RHS)*

In practical terms, before the design begins, the site for the construction of the RHF is selected and assessed, and this should include not only engineering-geological and seismic factors, but also meteorological characteristics of the area, including wind rose, hydrological characteristics, distance to settlements, transport connectivity and accessibility, possibilities for evacuation of personnel, population, material and cultural values, and the presence of other risky industries. These factors directly affect the radiation risk, because they determine the potential possibilities, directions and paths for the transfer of radioactive contamination, and the response time in the event of an accident [8–11].

Design is the most important stage because it is where the so-called "passive" protections are established, which do not depend at all or are minimally dependent on human intervention.

The three pillars of the international protection system are applied in the design:

- Justification (expediency): Any activity with sources of ionizing radiation must bring more benefits than harms.
- Optimization (As Low as Reasonably Achievable (ALARA) principle): Exposure levels should be "as low as reasonably achievable".

- Dose limitation: The project (designer) must ensure that even with certain deviations from normal work, no one will receive a dose above the maximum permissible dose for the relevant group (target category – personnel, population) [3]–[6].

The principle of justification requires that any activity involving sources of ionizing radiation should bring greater public, medical, scientific or economic benefit than the possible harm. The ALARA principle requires that exposures be kept as low as reasonably achievable, taking into account technical capabilities, costs and social impact. Dose limitations set an upper limit that the project must not allow to be exceeded for personnel and the public.

In principle, the design is based on the concept of defense in depth. These are a series of sequentially constructed physical barriers in the path of propagation of radioactive particles and ionizing radiation:

- Primary containment: Encapsulation of the radioactive substance;
- Biological protection: Use of materials that are a physical barrier and stop the spread of various radionuclide particles, electromagnetic and ionizing radiation.

Defense in depth practically combines several independent barriers: constructive containment of the radioactive substance, biological protection, controlled ventilation and filtration, emergency interlocks, physical protection, access control, redundancy of critical systems and technical means for radiation monitoring. Moreover, the failure of one protective barrier does not automatically lead to a risk of dangerous radiation exposure or uncontrolled spread of radioactivity, both in the area of the RHF and beyond its territory. [3, 5].

The designer, through the project, must divide the territory of the radiation hazardous site into:

- Controlled area: A place where special access and work regimes are required due to the risk of radiation;
- Surveillance zone: An area around the controlled zone where the radiation background is monitored, but the regime is lighter;

Outside the borders of the RHF, the following are also formed:

- Sanitary protection zone;
- Surveillance area.

Project zoning is directly related to sanitary and environmental protection. Controlled and supervised areas are defined inside the site, and outside it – a sanitary protection zone and a monitoring zone, when the nature of the site requires it. Zoning should provide a clear separation between workplaces with different radiation risk, personnel routes, radiation control points, sanitary locks, places for

storing personal protective equipment and points for decontamination (decontamination) [4, 12].

Already at the design level, the objects and parameters of radiation monitoring, the network of measurement points, the types of measuring instruments, the frequency of control, methodological support and the procedure for documentation are determined. At higher-risk objects, automated radiation monitoring systems must provide information in real time to a central point and, in certain scenarios, activate protective functions, for example, blocking a technological process, closing hermetic barriers or changing the ventilation mode [4, 7].

At the design stage of a radiation hazardous facility, the following is regulated:

- radiation monitoring sites;
- types of radiation monitoring;
- controlled parameters;
- permissible levels of controlled parameters;
- network of radiation monitoring points;
- frequency of radiation monitoring;
- technical means and methodological support for radiation monitoring;
- the composition of the necessary premises and the staff of workers performing radiation monitoring.

In order to obtain information about the state of the radiation situation in a radiation hazardous facility and in the environment, both during its normal operation and in the event of a radiation accident, the radiation monitoring system created at the facility as a whole must be in a mode that provides measurements of the parameters of the radiation situation in the following areas:

- dosimetric monitoring of personnel exposure;
- radiometric monitoring of skin contamination of personnel, property and transport within the restricted areas;
- monitoring the radiation situation in places where personnel work with radiation sources, including radioactive contamination;
- technological control;
- radiation monitoring of the environment.

The design should also include emergency management solutions: reliable notification, safe routes, shelters, backup power supply, communications, the ability to remotely control hazardous operations, and working conditions for emergency teams. In this sense, the design of a radiation hazardous facility is not just a construction and technical activity, but a complex system for preliminary risk management [8, 9, 13].

Ultimately, the design documentation should ensure traceability between the hazard analysis, the planned protective measures and the residual radiation risk. When a risk cannot be eliminated through engineering, technical and technological solutions, it should be managed through preventive and organizational measures, automated control and interlocks, personnel training, and strict adherence to emergency procedures. This avoids the formal design of individual systems without a common logic for integral safety [5, 6].

Today, modern design should rely on remote control (robotic arms, automated conveyors) to remove the person from areas with high background. Built-in automated radiation monitoring systems (ASRM) should provide a real-time signal to a central console and be able to automatically activate protective interlocks (e.g., stop ventilation or close hermetic doors) [13–15].

The analysis conducted suggests that the Preventive Approach is mandatory even at the design stage of the RHF, in order to create the most effective engineering protection, biological barriers, zoning of spaces and automated radiation monitoring systems. as the most modern means of radiation safety with minimal influence of the "human factor".

It is particularly important to understand that the design of a nuclear power plant is not only a technical, but also a strictly regulated process - each project must ensure compliance with a whole series of international, European and national regulatory documents before receiving a license from the Nuclear Regulatory Agency (NRA).

And last but not least, knowledge of the design zoning (controlled and supervised area) is essential for the rescue teams of the RHF and those of the Unified Rescue System (URS) in order to fully fulfill their obligations under the Internal and External Emergency Plans and to determine the safe limits of action in the event of a radiation accident.

B. Radiation safety and protection during the operation of radiation hazardous facilities

During operation, design decisions are transformed into a real system of technological discipline, instructions, control, maintenance and accountability. Operation of a RHF is a process in which technical designs are transformed into a living system of rules. Here, the main responsibility falls on the licensee (the organization managing the facility).

Each RHF operates on the basis of an approved comprehensive technological regulation. Any operation with ionizing radiation sources must be described in operating instructions, and deviations from the technological regime must be considered as a potential emergency factor [3, 4, 14].

Radiation monitoring of the working environment aims to assess the exposure of personnel, to detect deviations from the normal radiation environment and to prevent the spread of radioactive contamination. Usually, the radiation control process combines stationary automated systems, portable and mobile radiometers and x-ray meters,

laboratory analyses, taking various samples of air, water, soil, food, surfaces and technological environments, and materials, as well as proper documentation of the results of measurements and sample analyses in registers and databases in information systems [4].

In practice, the radiation situation can be assessed as normal, unfavorable, dangerous or extremely dangerous according to the exceedance of control levels, possible doses and the need for emergency interventions and protective actions.

This classification should not remain formal. It should be linked to pre-planned solutions: restricting access, stopping activities, increased monitoring, activating an emergency organization, notifying competent authorities, and attracting forces and resources from the Unified Rescue System [1, 8, 16].

Radiation monitoring of the environment has two important functions: informational and analytical. The informational function is aimed at early detection of emissions and changes in the radiation background. The analytical function clarifies the radionuclide composition, spatial distribution, trend and possible dose loads. In the event of an accident, the rapid determination of the boundaries of contamination, the dynamics of distribution, meteorological conditions, evacuation routes and access of emergency teams are of paramount importance [7, 17].

The technical maintenance of each element of the radiation monitoring and control systems is a very essential part of radiation safety. Faulty sensors, uncalibrated dosimetric equipment, compromised consumables and filters, poorly sealed barriers or faulty ventilation can turn an otherwise normal technological situation into a risk and emergency. Therefore, proper operation and maintenance, periodic inspections, calibration and independent control should be planned rhythmically according to technological requirements, documented and checked by competent control persons [4].

Decontamination is applied when radioactive contamination of personnel, various surfaces, equipment, vehicles, outdoor spaces and/or terrains is established. The choice of method depends on the type of radionuclides, the type of surface, the degree of radiation contamination, the time since the beginning of the incident and the possibility of this contamination spreading. The practical approach includes localization of contamination, restriction of access, measurement of radiation contamination, appropriate treatment of surfaces in the decontamination process, control measurement and subsequent management (treatment) of the collected waste as potentially radioactive. The aim is to reduce the dose load and prevent secondary contamination of the working and environmental environment [4, 17].

Radioactive waste management is an integral part of operational safety. It is necessary to minimize the waste generated and its separate collection, labeling, and marking, temporary storage, reporting, and transfer to a competent organization. This process should be planned during the design process, because the lack of sufficient

capacity for safe storage or incorrect classification of waste can create a new source of radiation risk [3, 8].

An essential element is the control of changes. Any change in a technological process, RHFm, ventilation scheme, measurement system, source used or storage method must be previously assessed in terms of the impact on the working and environmental conditions and on the radiation safety of the R&D facility. Without such control, even a small technical change can disrupt the design algorithms and logic of radiation safety and protection [3, 5].

Documentation has a very important evidentiary and management value. The registers (logs) for dose loads, the results of radiation monitoring, the results of checks on the technical serviceability and suitability of equipment, for the performed repair activities, training, briefings, for the conducted emergency drills and the transferred waste, allow traceability and timely detection of negative trends. In the event of an accident, it is these data that will show what the real risk was and whether all procedures were accurately implemented [4, 7].

The theoretical knowledge and practical experience acquired over the years give me reason to conclude that the decontamination of RHF of buildings and facilities, including nuclear power plants, was a particular challenge. In most cases, covered with bitumen, which easily adsorbs radioactive substances, the RHF are resistant to decontamination using traditional methods (using decontamination solutions). The most effective method for decontamination of RHF is the mechanical removal of bitumen coatings, which is associated with low productivity, especially in conditions of high external gamma radiation. In practice, various specialized decontamination solutions and methods for dry or wet cleaning were used, with the collected liquids being treated as liquid radioactive waste.

In addition, it is imperative to emphasize that:

- Safety during operation is based on strict compliance with labor and technological discipline, technological regulations (Art. 18 of the ASUNE) - any deviation from the instructions is a potential source of emergency risk.
- Radiation monitoring of the working environment and radiation risk management are continuous processes that ensure that the facility does not pollute the environment above permissible limits during its normal operation.
- Regular decontamination and technical maintenance of protection systems are a prerequisite against material fatigue and the unintended release of radioactivity into the working environment and the environment.

III. RESULTS AND DISCUSSION

A. Radiation safety and protection of personnel at radiation hazardous sites

Personnel are the most directly exposed group in the operation of radiation hazardous facilities. Their protection is based on a combination of individual dosimetric monitoring and control, clear rules and instructions, consistent medical supervision, continuous training, and the use of modern, functioning personal and collective protective equipment [4, 18].

Individual dosimetric control covers external and, when necessary, internal exposure. Personnel working in a controlled area must be provided with personal dosimeters, be kept on file and receive information about their own dose exposure. In emergency activities, additional dosimetric provision is appropriate because the conditions are dynamic and the risk of uneven exposure and dose overload is significantly higher [4, 12, 19].

Personal protective equipment is selected according to the specific hazard: external exposure, risk of radioactive contamination of the skin, inhalation risk, work with liquid or powdery contaminants, repair operations, confined space or elevated temperature. Personal protective equipment (PPE) does not replace engineered barriers, but is the last important protection against internal exposure of radionuclides and the spread of contamination [4].

Collective means of protection – shelters, filter-ventilation systems, protected control points, sanitary locks and checkpoints – provide protection for groups of people and maintain the manageability of the site in adverse conditions. They must be technically sound, checked, equipped with communications and taken into account the real number of people who can use them [18].

Medical supervision and training are critical to preventing various occupational injuries. Personnel without the necessary training, qualifications, instruction, or medical fitness should not be allowed to work to activities with sources of ionizing radiation. Training should be practical and include working with dosimetric equipment, proper donning and doffing of personal protective equipment (PPE), passing through a sanitary lock, actions in case of alarm and reporting deviations [3, 4].

Personnel protection is also a management issue. It is necessary for the managers of the RHF and those of the teams to maintain a higher level of safety culture, in which the reporting of small deviations - near-incidents and related technical problems is not formally sanctioned, but is used to improve the protection system. It should be clear that in radiation safety and protection, concealing a small, seemingly minor problem can become the cause of a serious subsequent emergency event [5].

Repair and unscheduled activities are particularly risky because they are often performed in a changed radiation environment, open technological systems, limited space, increased physical exertion and the need for sometimes very quick decisions. Therefore, such activities require a

preliminary and strict work program, a detailed dose estimate, a certain allowable downtime, the presence of a prepared equivalent backup team, means for backup communication and readiness for sudden cessation of work in case of a change in dosimetric readings [4, 20].

Psychological resilience also matters. In conditions of a radiation hazard alert, personnel must perform procedures calmly without panic or improvisation. This is achieved through continuous and repetitive training, clear management, practical training and trust between individual team members that measurements and instructions are reliable. A good safety culture reduces the likelihood of unauthorized departure, incorrect removal of PPE or transfer of contamination [5, 17].

An in-depth study of the activities in several RHF's showed that the personal discipline and compliance with radiation safety requirements of the personnel concerned, including the use (non-use) of PPE, as well as individual dosimeters, are not at a good enough level. For this reason, it is imperative to note that:

- Personnel protection is a combination of state and departmental dosimetric control and personal responsibility and discipline in wearing individual dosimeters.
- The correct selection of personal protective equipment (PPE), its technical condition and reliable operation are the last and practically the only barrier to internal exposure and radiation in a dusty or contaminated radioactive environment.
- Medical fitness and systematic training of personnel are not just a formality, but a legal instrument for decisively reducing occupational diseases and making mistakes in critical situations.

B. Radiation safety and protection of the population and the environment

One of the main measures to ensure radiation –safety of the population is the regulation of radiation exposure from various sources of ionizing radiation.

Control levels (doses, levels, activities, flux densities, etc.) are established in each specific radiation hazardous facility. Their values take into account the level of radiation safety achieved in the facility and provide conditions under which radiation exposure must be below permissible limits.

Furthermore, in order to prevent exceeding the permissible dose of anthropogenic radiation for the population (1 mSv/year) and to reduce radiation from anthropogenic sources –in accordance with the principle of optimization, as noted above, radiation norms (quotas) are established.

Protection of the population begins before the accident through planning, monitoring, awareness and readiness for rapid notification. In normal operation, the main tools are emission and immission control, dose limits, monitoring in the sanitary protection zone and the observation zone, as

well as periodic assessment of the environmental impact. In an accident, early warning, assessment of the situation, sheltering, access restrictions, evacuation, sanitation and control of water and food become the leading ones [4, 6, 8, 20, 21].

A radiation accident requires interaction and coordination between the licensee of the RHF, the Nuclear Regulatory Agency, health authorities, local authorities, the Directorate General of the National Safety and Health Protection, the police, medical structures, voluntary groups and other elements of the Unified Rescue System. Disaster Protection Plans. Part III, must contain realistic scenarios as close as possible to realistic scenarios, including the most adverse weather conditions, failure of connections and communications, difficult access to the RHF, the need for partial or complete evacuation and predicted prolonged radiation contamination [1, 3, 8, 9, 16].

Early warning and notification of the population is an essential preventive and psychological measure. The lack of clear information in many cases leads to panic, arbitrary evacuation, improper use of various preparations and distrust of institutions. Pre-prepared messages, access to Information about the radiation background, accurate and timely explanation of the measures and a single communication center reduce the risk of chaotic behavior. It is especially important to explain that iodine prophylaxis is applied only in cases of risk of radioactive iodine -131 and on the instructions of the competent medical authorities [7, 12, 19, 22].

Environmental protection requires an assessment of the impact on environmental factors - air, water, soil, vegetation, animals and the food chain. In the case of radiation pollution, sampling, laboratory analysis and control of pollution are organized, restriction of consumption of certain food products, control of water sources, management of contaminated foods and materials and monitoring of long-term effects. The relationship between radiation monitoring, sanitary control and the authorities responsible for food and agriculture is important [4, 7, 17].

In the context of defense and security, radiation-hazardous sites should also be considered as elements of critical infrastructure. Their protection includes not only technological safety, but also physical security, cybersecurity of monitoring and early warning and notification systems, resilient communications, redundant data exchange channels, and readiness for action in the event of combined threats. This is especially important for sites whose compromised resilience may have cross-border, socio-political, psychological, or long-term environmental effects [1, 7].

Annual exercises between site personnel, local authorities, voluntary groups and the Unified Rescue System forces are an important practical test of the effectiveness of the Disaster Protection Plan, Part III – Radiation Protection. The exercises should be comprehensive and test not only the formal announcement, but also the response time, the management method, the

exchange of data, the radiation protection of emergency teams, the organization of evacuation, special and sanitary treatment, laboratory control and the restoration of readiness for subsequent actions - the return to normal operation [1, 7, 17].

Disaster protection plans should be developed to anticipate different phases of the accident. In the early phase, the priority is on warning, hiding, restricting access and protecting emergency teams. In the intermediate phase, detailed radiation reconnaissance and mapping of contamination is carried out, medical surveillance, food and water control and waste management are organized. In the late phase, the main tasks are recovery, social support, long-term monitoring and informing the population about the residual risk [7, 17].

To be effective, the warning system should use all available and possible channels: sirens, mobile messages, the BG-ALERT public warning system (BG-ALERT), official websites, departmental networks and channels, local media, social networks and communication through city halls and other institutions. Messages should be short, unambiguous and applicable: what happened, which areas are affected, what citizens should do, what not to do and where they will get further information [22–24].

Special attention should be paid to vulnerable groups – children, the elderly, people with disabilities, hospitals, social services, schools and settlements with limited transport accessibility and connectivity. Routes, transport, accommodation, medical support and responsible persons should be determined in advance for them. A general evacuation scheme is insufficient when it does not take into account these practical limitations [1, 7].

After an accident, the recovery phase is no less important than the initial response. It includes the controlled return of the population, cleanup and decontamination, management of contaminated materials, economic support, damage assessment, and ongoing health surveillance. If this phase is not planned in advance, public pressure can lead to hasty decisions and new risks [7, 17].

It is important to emphasize that:

- Protection of the population is effective only when there is a well-established and functioning system for early warning and notification of management bodies, forces and means of the URS and a high degree of public awareness and preparedness of the population for behavior and action in conditions of radiation contamination.
- Of utmost importance for the radiation safety of RHF's and for the protection of the health and life of their personnel and the population of adjacent settlements, municipalities and districts is the development and maintenance of Disaster Protection Plans, Part III, as well as their permanent practice by conducting annual joint training exercises between the RHF staff, the volunteer formations and the

local authorities to practice coordination and interaction between them in emergency and crisis situations.

IV. CONCLUSION

Radiation safety in the design, operation and protection of personnel and the population is an inseparable process that requires a connection between high technologies, strict compliance with the legal framework and constant human discipline. The analysis shows that the Republic of Bulgaria has a regulatory system harmonized with European requirements, but its effectiveness depends on the actual implementation of the rules, on the maintenance of technical means and on the readiness for a coordinated response on the ground. In addition, the conducted field study and the analysis of the available information require the following main conclusions to be made:

- The majority of possible radiation risks can and should be reduced at the design stage of the RHF facility, through defense-in-depth, design zoning, automated monitoring and minimizing dependence on subjective human intervention.
- The personal responsibility of the personnel, their training and acquired culture of radiation safety, knowledge of radiation protection standards is the main thing against unwanted radiation incidents. Technological discipline, individual dosimetric control, proper use of PPE and medical supervision should be considered as a comprehensive and unified system.
- The relationship with the rescue services is key. The management bodies, the forces and means of the Unified Rescue System, and the volunteer formations must maintain skillful coordination with the licensed operator, because in the event of an accident, they are the ones responsible, and ensure the protection of personnel, the population, and the environment in the first critical hours after the accident.

In view of the overall improvement of radiation safety in the design and operation of RHF, it is advisable to do the following as soon as possible:

- To restore the integrity and modernize the network of radiation monitoring posts, including through the duty structures at the municipal and regional security councils, with the results of gamma background measurements being recorded, reported and summarized at the national level.
- To introduce integrated platforms for real-time data exchange between radiation hazardous sites, operational centers of the territorial units of the General Directorate of

Fire Safety and Population Protection, health authorities and local executive authorities.

- To expand the specialized training of the volunteer formations and emergency teams from the URS, with practical classes in decontamination, use of dosimetric equipment, personal protection and work in a controlled area.
- To restore and maintain a full-fledged system for repair, inspection and calibration of dosimetric equipment, as well as control over the serviceability and readiness for use of the available collective protective equipment.
- Maintain up-to-date disaster protection plans, Part III, at all levels, including worst-case scenarios, communications failure, complicated evacuation and prolonged contamination.
- To create easily accessible information resources for citizens regarding the gamma radiation background around large radiation-hazardous sites with a view to the correct behavior and action of the population in the event of a possible radiation accident.

REFERENCES

- [1] Disaster Protection Act. State Gazette, issue 102 of 19.12.2006, amended and supplemented.
- [2] Vladimirov V.A., Izmailkov V.I., Izmailkov A.V. Risk assessment and man-made safety management. Moscow: Delovai Express, 2002.
- [3] Law on the Safe Use of Nuclear Energy. State Gazette, No. 63 of 28.06.2002, amended and supplemented.
- [4] Radiation Protection Ordinance, adopted by Council of Ministers Decree No. 20 of 14.02.2018. State Gazette, issue 16 of 20.02.2018, amended and supplemented.
- [5] International Atomic Energy Agency. Fundamental Safety Principles. IAEA Safety Standards Series No. SF-1. Vienna: IAEA, 2006.
- [6] Council Directive 2013/59/Euratom of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionizing radiation. Official Journal of the European Union, L 13, 17.01.2014.
- [7] Buchinska-Simeonova, N., Radinov, A., Nikolova, D. Are doctors in Bulgaria ready to professionally assist victims of radioactive contamination in a terrorist act? Bulgarian Journal of Public Health, 2020, vol. 12, no. 2, pp. 54-65.
- [8] Ordinance on emergency planning and emergency preparedness in the event of a nuclear and radiation accident. State Gazette, issue 94 of 29.11.2011, amended and supplemented.
- [9] International Atomic Energy Agency. Preparedness and Response for a Nuclear or Radiological Emergency. IAEA Safety Standards Series No. GSR Part 7. Vienna: IAEA, 2015.
- [10] Dolchinkov N., M. Pavlov, Influence of meteorological elements in accidents in enterprises with radioactive elements or dangerous chemical substances in Bulgaria, 14th International Scientific and Practical conference Environment. Technology. Resources. Vide. Tehnologija. Resursi, 2023, ISSN 1691-5402, 1, pp. 49-54
- [11] Dolchinkov N., M. Pavlov, Study of the Influence of Winds in the Potential Contamination with Hazardous Substances as A Result of Man-Made Accidents, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume I, Print ISSN 1691-5402,

Online ISSN 2256-070X,

<https://doi.org/10.17770/etr2024vol1.7988>, pp 130-135

- [12] National Center for Radiobiology and Radiation Protection (NCRRP). Radioecological monitoring of working and living environment in the area of the ROO. Scientific monograph, Sofia, 2020.
- [13] Stoilov, G. A systematic approach to the management of preventive measures and early technological disclosure in radiation hazardous sites. Collection of reports from the International Forum "Radiation Safety in the Modern World", vol. 3, 2022, pp. 112-125.
- [14] Hristov, I., Petrov, N. Automated information systems for external radiation control and technological discipline in NPPs. Journal "First Atomic", issue 3, 2013, pp. 8-14.
- [15] Dolchinkov N., N. Nichev, Gamma-background radiation control systems as a factor of Bulgaria's national security, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume IV, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2024vol4.8225>, pp 83-88
- [16] Pavlov, M. Organizational and technical aspects of the interaction between the Unified Rescue System and critical infrastructure operators in radiation threats. Scientific journal Security and Defense, issue 2, 2023, pp. 45-58.
- [17] Regulation on the procedure for the construction, maintenance and use of collective protective equipment. Adopted by Council of Ministers No. 60 of 17.03.2009. State Gazette, issue 23 of 27.03.2009, amended and supplemented.
- [18] Regulation on safety in radioactive waste management. State Gazette, issue 76 of 30.08.2013, amended and supplemented.
- [19] International Commission on Radiological Protection. The 2007 Recommendations of the International Commission on Radiological Protection. ICRP Publication 103. Annals of the ICRP, 37(2-4), 2007.
- [20] Executive Agency for Environment (EAE). National System for Radiological Monitoring of the Environment in the Republic of Bulgaria: Radiation Characteristics of the Environment. Annual Report, Sofia, 2023.
- [21] Tsibryanski, R. Radioecological monitoring as a basic criterion and assessment for the safety of the population in the adjacent areas. Bulgarian Nuclear Society (BulAtom), 2017, pp. 15-28.
- [22] Regulation on the terms and conditions for the functioning of the National Early Warning and Disclosure System. State Gazette, issue 21 of 17.03.2020, amended and supplemented.
- [23] Regulation No. 8121z-413 of March 29, 2024 on the procedure for the establishment, maintenance, development and use of the BG-ALERT system for the dissemination of warning messages to the population. State Gazette, issue 32 of 09.04.2024.
- [24] Dolchinkov N., State of the population disclosure systems in the changing radiation situation in Bulgaria, 12th International Scientific and Practical conference Environment. Technology. Resources. ISSN 1691-5402, Vol 1, 20-22.06.2019, Rezekne, Latvia, pp. 54-58

Mediation as a Risk Management Instrument Reframing Organizational Conflict as a Missing Structural Element in Erm Frameworks

Georgi Dimitrov

University of Agribusiness and Regional Development

Plovdiv, Bulgaria

gdimitrov@uargd.bg

Abstract: In contemporary organizations, risk is increasingly generated internally rather than imposed externally. Among the most underestimated sources of such internal risk are unresolved conflicts, communication breakdowns, and escalation dynamics within and between stakeholders. This paper advances the argument that mediation should be reframed from a purely legal or alternative dispute resolution (ADR) mechanism into a structured instrument within enterprise risk management (ERM) systems. More specifically, it argues that mediation is a missing structural element in ERM frameworks. By integrating mediation into the risk control architecture, organizations can transform conflict from a destabilizing factor into a managed process. The paper proposes a conceptual model positioning mediation as a distinct risk control layer and explores its implications for organizational resilience, decision-making speed, and value preservation.

Keywords: Mediation; Risk Management; Enterprise Risk Management; Organizational Conflict; Risk Control; ADR; Operational Risk; Reputational Risk.

I. INTRODUCTION

Traditional approaches to enterprise risk management have historically focused on external threats including market volatility, regulatory uncertainty, cyber threats, supply chain disruption, and geopolitical instability. While these threats remain significant, both empirical observation and organizational practice increasingly demonstrate that a substantial proportion of operational, reputational, and strategic risks originate within the organization itself [1], [2].

These internally generated risks frequently emerge from stakeholder misalignment, leadership friction, communication breakdowns, competing incentives, and unresolved organizational conflict. Unlike external threats, such relational risks often evolve gradually, remain difficult to quantify in their early stages, and become

visible only after they have already materialized into measurable organizational loss.

Despite their significance, organizational conflicts are rarely treated as structured risk variables within formal enterprise risk management systems. Instead, they are commonly delegated to human resources departments, compliance units, legal departments, or external dispute resolution mechanisms only after escalation has occurred.

This reactive paradigm creates a critical structural vulnerability. At the point of formal legal escalation, organizations often lose procedural control, strategic flexibility, and the ability to preserve stakeholder relationships.

This paper challenges this paradigm by proposing mediation as a proactive and structured risk management instrument. More specifically, it argues that mediation represents a missing structural control layer within existing enterprise risk management architectures.

The study pursues four primary research objectives. First, it examines whether contemporary Enterprise Risk Management (ERM) frameworks explicitly recognize organizational conflict as a measurable internal risk variable. Second, it evaluates the functional characteristics of mediation as a preventive organizational control mechanism capable of interrupting escalation dynamics before operational and reputational losses materialize. Third, the study identifies structural deficiencies within existing risk management architectures regarding relational and interpersonal risks. Finally, the paper proposes an integrated multi-layer organizational model positioning mediation as a dedicated structural control layer within ERM systems.

In addition to these objectives, the study seeks to contribute to the growing interdisciplinary discussion

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.211>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

concerning organizational resilience, governance adaptability, and the strategic management of internal volatility under conditions of uncertainty.

Contemporary Enterprise Risk Management literature has significantly expanded during the last two decades, particularly in areas such as strategic risk governance, operational resilience, cybersecurity, compliance, and reputational exposure. Nevertheless, despite this conceptual evolution, relatively limited scholarly attention has been devoted to organizational conflict as an independent measurable risk vector.

Most existing ERM frameworks approach conflict indirectly through secondary indicators such as employee turnover, litigation, operational inefficiency, governance disruption, or reputational deterioration. As a result, organizations frequently address the consequences of escalation rather than the underlying relational mechanisms that generate systemic instability.

Simultaneously, mediation literature has traditionally framed mediation primarily as a legal or alternative dispute resolution (ADR) mechanism. While mediation research extensively examines negotiation dynamics, communication restoration, and dispute resolution efficiency, comparatively little attention has been paid to mediation as a proactive organizational control instrument integrated within enterprise risk architectures.

This study therefore addresses an interdisciplinary research gap located at the intersection of organizational conflict management, mediation theory, and enterprise risk governance. The paper proposes that mediation should be reconceptualized not merely as a post-conflict intervention mechanism, but as a structural component of organizational risk stabilization.

The interdisciplinary nature of the present study creates a specific research limitation regarding the availability of directly applicable academic literature. While substantial bodies of scholarship exist independently within Enterprise Risk Management (ERM), mediation studies, organizational psychology, and conflict management, relatively limited research has examined mediation specifically as an integrated structural component of enterprise risk governance systems.

Most existing mediation literature focuses predominantly on legal dispute resolution, negotiation processes, or Alternative Dispute Resolution (ADR) frameworks, whereas ERM literature traditionally concentrates on financial, operational, compliance, strategic, and cybersecurity risks. Consequently, the intersection between mediation and enterprise risk architecture remains comparatively underexplored in contemporary academic research.

For this reason, the present study adopts an interdisciplinary theory-building approach aimed not at reproducing established models, but at identifying conceptual gaps and proposing an integrative analytical framework capable of connecting organizational conflict dynamics with internal risk stabilization mechanisms.

The copyright of articles is transferred to the Rezekne Academy of Technologies. Articles will be published under [*Creative Commons Attribution 4.0 International License*](#).

II. MATERIALS AND METHODS

This research applies an exploratory qualitative methodology based on three complementary analytical approaches.

First, a comparative analysis of established enterprise risk management frameworks was conducted, focusing primarily on frameworks developed by the Committee of Sponsoring Organizations of the Treadway Commission and the International Organization for Standardization [1], [2].

The purpose of this analysis was to identify whether relational and interpersonal conflicts are explicitly recognized as measurable risk categories and whether existing frameworks provide operational mechanisms for conflict containment before escalation.

Second, a systematic review of mediation and conflict resolution literature was conducted in order to evaluate the functional characteristics of mediation as a control mechanism within complex organizational environments [3]–[6].

Third, conceptual organizational modeling was employed to synthesize both domains of knowledge into an integrated enterprise risk architecture.

The study is theory-building in nature and aims to identify structural deficiencies within current enterprise risk management systems while proposing a practical conceptual solution.

The present research should be understood primarily as a conceptual and theory-building study rather than a statistically driven empirical investigation. Its primary objective is to develop an analytical framework capable of reframing organizational conflict as a measurable component of internal enterprise risk architecture.

Accordingly, the study prioritizes conceptual integration, structural analysis, and interdisciplinary synthesis over quantitative generalization. The illustrative organizational scenarios included in the paper serve as applied conceptual demonstrations intended to support the practical plausibility of the proposed model.

Future empirical research may further validate the framework through sector-specific case studies,

comparative institutional analysis, and quantitative assessment of conflict-related organizational indicators.

III. RESULTS AND DISCUSSION

A. Enterprise Risk Management Frameworks and Structural Gaps

Enterprise risk management frameworks have significantly evolved during the last two decades. Modern frameworks emphasize integration of risk management into governance, strategic planning, operational decision-making, and performance management [1], [2].

However, the comparative analysis reveals a notable structural limitation.

While frameworks successfully address:

- Strategic risks
- Financial risks
- Compliance risks
- Operational risks
- Cybersecurity risks
- Reputational risks

they rarely identify organizational conflict as an independent measurable risk vector.

Conflict typically appears only indirectly through secondary manifestations such as employee turnover, litigation exposure, productivity loss, governance breakdown, or reputational deterioration.

As a result, organizations frequently manage symptoms rather than root causes.

This omission creates a systemic blind spot in enterprise risk architectures.

B. Organizational Conflict as a Risk Vector

The literature in organizational psychology and behavioral management recognizes conflict as both a potential source of innovation and a potential source of dysfunction [5].

However, when unmanaged, organizational conflict tends to follow a predictable escalation trajectory:

Conflict → Escalation → Risk Materialization → Loss

At each escalation stage, organizations experience increasing exposure in several dimensions:

- *Operational Exposure*
 - Project delays
 - Reduced productivity
 - Breakdown in decision execution
 - Resource inefficiency
- *Financial Exposure*
 - Legal costs
 - Lost business opportunities
 - Increased employee turnover costs
 - Contractual disruption
- *Reputational Exposure*
 - Loss of stakeholder confidence
 - Negative media attention
 - Reduced investor confidence
- *Strategic Exposure*
 - Loss of key partnerships
 - Governance instability
 - Strategic decision paralysis

By the time conflict reaches formal litigation or regulatory intervention, organizations effectively transfer control over process and outcome to external actors.

This transfer of control represents not only a legal risk but a strategic vulnerability.

C. Mediation as a Missing Structural Control Layer

The analysis suggests that mediation should not be viewed exclusively as an alternative dispute resolution mechanism, but rather as a proactive organizational control instrument.

Mediation possesses several characteristics that distinguish it from traditional reactive mechanisms:

- Confidentiality
- Voluntary participation
- Speed of intervention
- Preservation of stakeholder relationships
- Process flexibility
- Internal ownership of outcomes

These characteristics make mediation particularly suitable for integration within enterprise risk architectures.

This paper therefore proposes mediation as a missing structural control layer positioned between conflict detection and reactive intervention.

D. Proposed Multi-Layer Risk Architecture

The proposed organizational architecture consists of four integrated layers.

1) Preventive Layer

This layer includes:

- Organizational culture
- Governance frameworks
- Leadership development
- Compliance mechanisms
- Communication protocols
- Conflict awareness training

Its primary objective is prevention of relational risk formation.

2) Detection Layer

This layer focuses on early identification of emerging conflict signals, including:

- Communication breakdowns
- Behavioral anomalies
- Stakeholder friction
- Team polarization
- Escalating grievances

Detection mechanisms may include:

- HR analytics
- Internal reporting channels
- Risk indicators
- Management escalation reporting

3) Mediation Layer (Proposed Structural Element)

This study identifies mediation as the currently missing structural layer.

Within this architecture, mediation performs critical control functions:

- Interrupts escalation dynamics

- Restores communication channels
- Preserves decision autonomy
- Reduces uncertainty
- Protects relational capital
- Maintains organizational control over outcomes

Unlike litigation, mediation preserves internal procedural ownership.

4) Reactive Layer

This layer includes:

- Litigation
- Arbitration
- Regulatory intervention
- Crisis communication
- Reputation management
- Damage control

While necessary, these mechanisms operate only after measurable risk has already materialized.

E. Mediation as a Risk Transformation Mechanism

The conceptual model demonstrates that mediation fundamentally alters the trajectory of risk development.

- *Without Mediation:*

Conflict → Escalation → Loss

- *With Mediation:*

Conflict → Controlled Process → Managed Outcome → Value Preservation

This transformation illustrates mediation not merely as a resolution mechanism, but as an operational process for converting relational volatility into controlled organizational outcomes.

F. Strategic Implications

Organizations that institutionalize mediation within their enterprise risk management systems may achieve several strategic advantages:

- Reduced operational volatility
- Faster decision cycles
- Lower legal dependency
- Improved stakeholder retention
- Enhanced organizational resilience
- Greater adaptability under pressure

Conversely, organizations lacking such a structural layer remain exposed to uncontrolled escalation, delayed intervention, and amplified loss magnitude.

From a risk management perspective, the absence of mediation should itself be recognized as a measurable systemic risk factor.

A. Illustrative Organizational Scenarios

Although the present study is conceptual in nature, several practical organizational scenarios illustrate the applicability of the proposed model.

1) Scenario 1: Executive Leadership Conflict and Strategic Paralysis

In large organizations, strategic disagreements between executive stakeholders frequently evolve into prolonged decision paralysis. In such situations, communication channels deteriorate, internal coalitions emerge, and operational execution becomes delayed. Traditional risk management systems often identify only the secondary manifestations of the problem, such as project delays, governance instability, or financial underperformance.

The proposed mediation layer enables early intervention before formal escalation occurs. By restoring controlled communication and preserving procedural ownership of the decision-making process, mediation reduces escalation intensity and preserves organizational adaptability.

2) Scenario 2: Cross-Department Operational Conflict

Operational conflicts between departments with competing priorities, such as compliance divisions and operational management teams, may generate significant organizational friction. Escalation frequently results in reduced efficiency, delayed implementation processes, increased employee turnover, and heightened legal exposure.

Within the proposed architecture, mediation functions as a stabilization mechanism capable of interrupting escalation trajectories before external legal or regulatory intervention becomes necessary. This preserves institutional flexibility and reduces operational volatility.

3) Scenario 3: High-Risk Organizational Environments

In high-risk sectors such as healthcare, critical infrastructure, or emergency management systems, unresolved organizational conflict may directly affect operational continuity and decision reliability. Communication breakdowns between administrative and operational personnel may create systemic vulnerabilities capable of amplifying existing organizational risks.

The proposed mediation framework may therefore contribute not only to dispute resolution, but also to organizational resilience by preserving communication integrity and maintaining coordinated decision-making under conditions of pressure.

These scenarios demonstrate that mediation may operate not simply as a dispute resolution mechanism, but as an organizational process for transforming relational volatility into controlled operational outcomes.

B. Research Limitations

Several limitations of the present study should be acknowledged.

First, the research is conceptual and exploratory in nature and does not include large-scale quantitative validation. The objective of the study is theory development and structural reframing rather than statistical generalization.

Second, the proposed model has not yet been empirically tested across multiple organizational sectors or institutional environments. Consequently, the effectiveness of mediation as an integrated ERM control mechanism requires further empirical investigation.

Third, the interdisciplinary nature of the study combines concepts from enterprise risk management, organizational psychology, governance theory, and mediation studies. While this interdisciplinary integration represents one of the strengths of the paper, it also introduces methodological complexity regarding measurement standardization and comparative evaluation.

Future research should therefore focus on empirical validation of the proposed architecture through organizational case studies, comparative institutional analysis, and quantitative assessment of mediation-related outcomes such as escalation reduction, operational continuity, stakeholder retention, and organizational resilience.

The proposed model may be applied within multiple organizational environments where internal communication dynamics and stakeholder coordination directly influence operational stability.

Potential areas of application include:

- corporate governance systems;
- compliance and ethics structures;
- healthcare administration;
- critical infrastructure organizations;
- public administration institutions;
- multinational organizational environments;
- crisis management and emergency coordination systems.

Within such environments, mediation may function as an internal stabilization mechanism capable of reducing escalation intensity, preserving communication continuity, and limiting operational disruption resulting from unresolved organizational conflict. The framework may also support the development of conflict-sensitive risk indicators within broader Enterprise Risk Management systems.

IV. CONCLUSIONS

This study argues that mediation should be repositioned from a post-dispute legal mechanism into a proactive structural component of Enterprise Risk Management systems.

The research demonstrates that contemporary ERM frameworks contain a significant structural blind spot regarding relational and interpersonal conflict as measurable internal organizational risk vectors. Existing risk architectures predominantly address the secondary consequences of escalation, including operational disruption, reputational damage, litigation exposure, and governance instability, while insufficiently addressing the underlying communication and relational dynamics that generate such outcomes. The proposed multi-layer organizational model introduces mediation as a dedicated control layer situated between conflict detection and reactive intervention. Within this framework, mediation functions not merely as a resolution mechanism, but as an operational process capable of interrupting escalation trajectories, restoring communication integrity, preserving stakeholder relationships, and maintaining organizational control over decision-making processes.

From a theoretical perspective, the study contributes to the ongoing evolution of Enterprise Risk Management by integrating mediation into the broader architecture of organizational resilience and internal risk stabilization. The paper expands the conceptual understanding of risk by reframing unresolved conflict as a measurable source of organizational volatility.

From a practical perspective, the proposed framework may assist organizations in reducing escalation-related losses, improving governance adaptability, preserving relational capital, and strengthening internal resilience mechanisms under conditions of uncertainty.

The study also suggests that the absence of structured mediation mechanisms should itself be interpreted as an indicator of organizational vulnerability within contemporary organizational environments.

Future research should focus on empirical validation of the model through quantitative assessment of mediation's impact on conflict escalation speed, operational continuity, litigation reduction, stakeholder retention, and long-term organizational resilience. Unlike traditional mediation studies focused primarily on dispute resolution, the present research contributes by reframing mediation as a structural organizational risk control mechanism embedded within enterprise governance architecture.

The limited availability of directly integrated academic models combining mediation and Enterprise Risk Management further demonstrates that this field remains at an early stage of interdisciplinary development. Consequently, the present study may serve as a foundation for future theoretical and empirical research examining conflict-sensitive risk architectures within contemporary organizations.

Declaration of AI Use and Author Contribution **Author's Original Contribution**

The core concepts, the proposed multi-layer risk architecture, and the conceptual transformation models presented in this paper are the original work of the author. These ideas are rooted in extensive research into the systemic limitations of traditional enterprise risk management (ERM) frameworks - specifically their failure to address interpersonal and relational risks as measurable variables. The repositioning of mediation as a proactive risk control layer arises from the author's professional experience and analysis of how unresolved organizational conflict serves as a primary vector for operational and reputational loss.

Use of Artificial Intelligence

Text Enhancement: Generative AI was employed solely as a linguistic and structural tool to improve the readability, flow, and grammatical precision of the manuscript. The AI did not generate new ideas or alter the underlying theoretical framework.

REFERENCES

- [1] Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management: Integrating with Strategy and Performance, 2017.
- [2] International Organization for Standardization, ISO 31000: Risk Management—Guidelines, Geneva, Switzerland, 2018.
- [3] C. Moore, The Mediation Process: Practical Strategies for Resolving Conflict, 4th ed. San Francisco, CA: Jossey-Bass, 2014.
- [4] R. Fisher, W. Ury, and B. Patton, Getting to Yes: Negotiating Agreement Without Giving In, 3rd ed. New York, NY: Penguin Books, 2011.
- [5] C. K. W. De Dreu and M. J. Gelfand, The Psychology of Conflict and Conflict Management in Organizations. New York, NY: Taylor & Francis, 2008.
- [6] J. Bercovitch, V. Kremenjuk, and I. Zartman, The SAGE Handbook of Conflict Resolution. London: Sage Publications, 2008.
- [7] D. Hillson, Extending the Risk Process to Manage Opportunities. London: Gower, 2002.
- [8] J. Lam, Enterprise Risk Management: From Incentives to Controls. Hoboken, NJ: Wiley, 2014.
- [9] P. Hopkin, Fundamentals of Risk Management. London: Kogan Page, 2018.

Integration of Digital and Artificial Intelligence Solutions in Mental Healthcare

Vihra Dimitrova

Faculty of Telecommunications and Management
University of Telecommunications and Post
Sofia, Bulgaria
v.dimitrova@utp.bg

Abstract— The current paper explores the transformative role of the digital tools and artificial intelligence in the field of mental healthcare. As global demand for psychological support outpaces the availability of human specialists, digital and AI-driven solutions offer a scalable bridge to fill this gap. The study examines the transition from traditional diagnostic methods to data-driven, predictive models. The research utilizes a comparative analysis of leading AI therapeutic platforms and evaluates the technical foundations of digital phenotyping and Natural Language Processing. Furthermore, the paper analyses the legal implications of the European Union's AI Act on high-risk medical algorithms.

Keywords— AI, digitalization, digital phenotyping, mental health.

I. INTRODUCTION

The rapid development of new information and communication technologies, which we have witnessed over the past decade, is leading to a completely new dynamic and complex reality within which political, economic and social developments unfold. The digital revolution is changing the world at an unprecedented pace. The use of new technologies and digital devices has begun to enter people's personal and professional lives at an ever-faster pace, and institutions have had to change in a timely manner to respond to the new conditions [1].

In the modern world, technology is at the forefront of many sectors, shaping our daily lives and transforming traditional norms. One area that is undergoing significant evolution due to digital intervention is mental health care. The rise of digital solutions in this space is opening up new avenues for providing support, improving accessibility and potentially revolutionizing mental health outcomes.

The global health crisis of the past two years has confirmed the need to accelerate digital transformation in all economic and societal sectors, including healthcare.

According to the World Health Organization, nearly 1 billion people worldwide suffer from a mental health disorder, resulting in enormous personal suffering and socio-economic costs [2]. Mental health problems are

increasing at an alarming rate worldwide, and unfortunately, the COVID-19 pandemic has contributed to exacerbating the problems.

The disruption caused by the pandemic is unprecedented, and the resulting economic and social measures have led to a huge change in lifestyles. The pandemic situation and the measures introduced have further exacerbated the crisis in the mental health of the population. Episodes of anxiety and depression have increased by up to four times during the pandemic.

Nowadays, digital technologies, platforms and applications become a reality within the delivery of mental health pathways. Number of these solutions are now part of a broader healthcare landscape focused on improving population mental health and the delivery of health services. Nevertheless, challenges remain in how digital is defined; how innovation, research and development are supported; and how transparency is provided about the role of digital mental health.

The global healthcare system is facing another unprecedented challenge posed by the escalating incidence of mental disorders and the chronic shortage of qualified personnel. In this context, artificial intelligence (AI) is emerging not just as an auxiliary tool, but as a fundamental technological and epistemological force capable of replicating and extending the cognitive functions of the human mind, including learning from experience, understanding linguistic nuances, and solving complex diagnostic tasks [3]. This paper analyses the broad impact of the digital and AI-driven solutions on mental health care, examining the technological mechanisms, the clinical efficacy of contemporary interventions, and the legal imperatives that shape the future of the mental health care.

II. MATERIAL AND METHOD

The material includes a review of the main features of the digital platforms used in mental healthcare, fields of application, limitations and legal regulation. The following scientific methods were used in the research process -

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.119>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

analysis and synthesis, descriptive and comparative analysis.

III. RESULTS AND DISCUSSION

A. *Main features and fields of application of digital tools and AI-driven solutions in mental health care*

Digital health in general includes mobile health, health information technology, wearable devices, telemedicine and personalized medicine [4]. Specifically for the field of mental health, digital health is defined as a therapeutic intervention for mental health delivered via a website, smartphone or tablet application [5].

Digital mental health is defined as support for emotional needs delivered via computer technology (apps, video visits via smartphone or computer, videos on demand and text messages on a smartphone). These tools can be clinical (providing a diagnosis and/or treatment plan) or wellness-based (subclinical). The use of benefits that include a digital component via a smartphone or computer is becoming increasingly common.

Digital technologies like smartphones, wearables, and web platforms are the foundation for collecting data. Meanwhile, artificial intelligence analyses the data to provide care that's tailored to the individual needs. This combination of digital tools and AI works together in a way that enhances each other's strengths. Digital tools help gather all sorts of information, and then AI steps in to make sense of it all, leading to more precise and personalized care for patients.

Digital mental health tools vary considerably in their target audience, delivery method, psychological theory, and intensity. Tools can span the continuum of care, from prevention to crisis management. Some tools are aimed at patients with a clinical illness, while others offer only educational content. Some categories include: self-monitoring; cognitive enhancement; skill acquisition; social support; symptom tracking; and passive data collection.

Types of digital mental health care can be categorized into several areas:

- Prevention;
- Assessment;
- Treatment;
- Crisis interventions;
- Post-treatment management;
- Ongoing monitoring.

Digital mental health tools are mobile applications designed to help users improve their emotional well-being, become more aware, and cope with some common problems. Some of the digital mental health solutions allow users to access online therapy or psychiatric help; others are aimed at starting a meditation practice, managing stress and anxiety, or improving sleep quality. The best digital mental health solutions are accessible, easy to use, and well-designed, with few technical issues. High-quality digital therapeutic tools remove some of the common barriers to mental health care, while applications to

increase concentration and attention lead to high productivity.

Digital tools in mental health care are aimed at both prevention and the acquisition of new skills and self-help in relation to an existing problem. There are many tools on the market, with different ways of working and intensity. Some of the most common applications are used to:

- Practicing different types of meditation and mindfulness. Various digital tools are developed with the scope of practicing mindfulness techniques and guided meditation sessions.
- Learning coping skills. Some mental health applications use different activities and online worksheets helping users in developing key skills, such as functional ways to cope with stress and improve attention and concentration.
- Breathing practices. They allow users to learn and practice various breathing techniques on their own.
- Stress management. Many apps focus on preventing and managing stress, which affects a large portion of the world's population.
- Addiction recovery. They provide progress monitoring and support during the process of overcoming various types of addictions.
- Anxiety and depression. They offer the opportunity for remote meetings and therapy with a qualified therapist. Along with stress management apps, tools for overcoming anxiety and depression are the most sought-after and most commonly used.
- Sleep problems. There are applications that are suitable for insomnia and restless sleep. Features such as dream sequences, guided imagery, audio narration stories, soothing music, and nature sounds are used to aid in falling asleep and staying asleep.

While traditional mental health applications often offer static content, AI transforms these tools into adaptive systems like chatbots and Ecological momentary interventions. Digital platforms like Woebot and Wysa use natural language processing to conduct dialogue and apply cognitive behavioural therapy techniques in real time. AI analyses the user's context through sensors and sends therapeutic prompts at the exact moment they are needed (e.g., when high stress is detected through heart rate).

Traditional therapy is based on building strong relationships with patients. The therapist takes the time to listen, understand, and support their patients. However, traditional therapy models are expensive, difficult to plan, and cannot be scaled. Emerging digital mental health solutions offer on-demand therapy at any time. Text communication is the predominant mode of interaction; some companies use software to automate responses, while others promote self-help tools.

The global health crisis has fundamentally changed the patterns of demand and supply of health care. The challenge for health care professionals is to determine which digital solutions for mental health are effective and will benefit their patients. Modalities range widely and may include telephone, videoconferencing, computer-based interventions, mobile phone-based interventions, patient monitoring sensors, social media, virtual reality, and games. The offerings are typically divided into three main intensity categories: self-directed use of online content; hybrid forms of online content and contact with a therapist; and extended therapy using videoconferencing, telephone, text messaging, and/or email between in-person psychotherapy sessions. Therapies used may include: Cognitive behavioural therapy, Dialectical behaviour therapy, stress management, and attention and concentration enhancement. With the advent and widespread use of new technologies, the general interest in digital solutions for mental health has grown significantly [4].

Both providers and researchers note that digital tools can provide prevention as well as treatment. Prevention can be achieved through screening and early intervention “to reduce risk factors and build psychological resources” [6] and “passive monitoring of psychological states that can alert consumers and providers to acute and chronic stressors predisposing to subsequent clinical disorders” [7].

B. Technology architectures and multimodal approaches in digital mental healthcare

The transition to more precise mental healthcare relies on artificial intelligence's ability to analyse complex data and find patterns that remain invisible to traditional diagnosis methods. This process involves the integration of multimodal datasets spanning neuroimaging, electrophysiological signals, electronic health records. This combined data, often referred to as “digital phenotyping,” helps to create a more detailed picture of a person's health [8]. In modern psychiatry, the concept of “digital phenotyping” is gaining ground. This is the concept of instantaneous and passive data collection from personal devices, using the typing kinetics and voice prosody. Changes in the speed of typing messages and the frequency of typos can signal cognitive decline or a manic episode.

By using AI to analyse all this data, clinicians are able to find patterns that they might not have seen otherwise, which can lead to more accurate diagnoses and better treatment plans. The goal is to use this information to provide more personalized care for patients, taking into account their unique characteristics and needs. Unlike traditional questionnaires that rely on subjective responses, AI uses convolutional neural networks to analyse facial expressions and micro-mimics during an interview and recurrent neural networks for time series analysis (e.g. changes in sleep quality over a month), allowing for prediction of relapse in bipolar disorder.

TABLE 1 TECHNOLOGICAL ANALYSIS OF THE MENTAL HEALTH STATUS

Technological domain	Methods and purpose	
	Specific methods	Clinical purpose
Electroencephalography	spectral density, functional connectivity	differential diagnosis of depression and psychosis
Electrocardiography	heart rate variability	assessment of psychophysiological stress and anxiety
Natural language processing	sentiment analysis, topical modeling	detecting cognitive markers in speech and text
Digital phenotyping	passive smartphone data analysis	tracking relapses and changes in activity
Genetic and blood biomarkers	multivariate integration	personalized choice of pharmacotherapy

Electroencephalographic (EEG) and electrocardiographic (ECG) data are emerging as critical sources for machine learning. EEG-based models use spectral analysis and functional connectivity studies to identify specific biomarkers for depression and schizophrenia. In parallel, heart rate variability analysis provides objective data on the state of the autonomic nervous system, reflecting the levels of stress and the individual's capacity for emotional regulation [9]. By combining this information, AI can act as an early warning system, spotting signs of decline that may not be noticeable to the patient or their therapist until later on. This can happen even before the symptoms become severe enough to be considered a clinical issue.

Among the most important AI techniques used are machine learning, deep learning, natural language processing (NLP), and multimodal AI and they “have shown promise in enhancing mental health services” [8]. There are different technological domains, using specific methods in order to provide data, analyse it and assess the user's condition in regard to mental health status (Table 1).

One of the most demanding areas for the application of machine learning is the prediction of suicidal behaviour and self-harm. Traditional clinical assessments in this area show limited accuracy that has not improved significantly in recent decades [10]. In contrast, predictive algorithms trained on real clinical data have demonstrated the ability to generate individual predictions with high precision [11].

Research has found that using a mix of structured data from electronic health records, like patient info, past diagnoses, medications, and unstructured text from clinical notes, gives the best outcomes. Using natural language processing allows the mining of terms and emotions from free text, which significantly improves the detection of suicidal thoughts, including specific groups such as pregnant women or patients discharged from hospital. For example, NLP can help find patterns in clinical notes that might suggest someone is at risk of suicide, even if they don't explicitly say so. By combining this with other data, like demographics and medical history, we can get a more

complete picture of a patient's risk factors and provide better care [12]. Despite their high accuracy, analysis of these models reveals critical challenges related to the “data noise” and the need for external validation [11]. For example, NLP models could generate false signals due to specific writing habits of clinicians or the use of negations, like “the patient is not suicidal”, which requires precise filtering and contextual understanding [10].

The development of conversational agents (chatbots) marks a new era in the accessibility of psychosocial support. These tools offer anonymity, and scalability, that make them convenient to address stigma and overcome geographical barriers. The clinical effectiveness of AI chatbots is demonstrated by a number of meta-analyses confirming that AI-based interventions achieve small to moderate effects in reducing symptoms of depression, anxiety, and stress. A recent randomized controlled trial published in *JIMR Mental Health*, demonstrated that a digital program combining AI conversational agents with clinical supervision achieved outcomes that were almost equal to traditional cognitive behavioural therapy delivered face-to-face or via chat with a therapist [13]. The same significant result suggests that the technology could reduce clinician time by up to 8 times while maintaining therapeutic effectiveness. Some of the digital mental health solutions have clinical evidence and have been analysed along with their key functionalities, target group, level of autonomy and validation (Table 2).

TABLE 2 ANALYSIS OF THE MAIN DIGITAL MENTAL HEALTH APPLICATIONS

Characteristic	Platform		
	<i>Woebot</i>	<i>Wysa</i>	<i>Youper</i>
Basic methodology	Cognitive behavioral therapy	Cognitive behavioural therapy, Dialectical behaviour therapy, Yoga, Meditation	Cognitive behavioural therapy, Acceptance and commitment therapy
Technological approach	Structured dialogue - rule-based and NLP	Hybrid model – AI and access to human therapist	Personalized emotional monitoring - sentiment analysis
Target group	Depression, anxiety, postpartum depression	A wide spectrum from stress to chronic pain	Users with mood swings and social anxiety
Clinical evidence	Strong Multiple randomized controlled trials, 22% reduction in depression scores (PHQ-9)	High Partnerships with NHS, UK, improved engagement through empathetic interface	Moderate The focus is on user experience, reduction in anxiety symptoms
Level of autonomy	Fully autonomous	Escalation to a person at risk	Referral to professional help

It is evident that the most popular digital applications in the mental healthcare differ in their functionalities, technological approach, target group and clinical evidence. Other platforms, like Noah AI and Replika, are used for voice therapy, crisis intervention and emotional companionship.

C. *Digital therapeutic alliance and humanistically oriented artificial intelligence*

A central question in contemporary psychotherapy is whether and how the traditional concept of the therapeutic alliance—the relationship between therapist and patient—can be transferred to the digital realm [14]. The emerging framework of the digital therapeutic alliance explores the mechanisms of empathy, trust, and collaboration in the context of the interaction between an individual and a machine [15].

Research using adapted versions of the Working Alliance Inventory (WAI-SR) identifies five main dimensions of the digital therapeutic alliance:

- Flexibility – represents the ability of the user to choose the style of the dialogue — whether to be led by a chatbot or to initiate topics themselves.
- Goal and task alignment – consists of mutual understanding between the user and the algorithm about the steps needed to achieve therapeutic progress.
- Emotional experience – perceiving the feeling of warmth, empathy, and non-judgmental presence from the AI agent.
- Openness and self-disclosure – represent the extent to which the anonymity of the digital environment encourages the sharing of deeply personal issues.
- Responsibility – encompass the sense of commitment to the process that the application induces.

Critics highlight the existence of a “genuineness gap”—since artificial agents lack consciousness or moral responsibility, their empathic expressions remain ontologically “hollow,” which can undermine the deep socio-emotional functions of therapy for certain patients [16].

The integration of AI into mental healthcare should not be considered in isolation from psychological theory. The “common factors model” or contextual model argues that the success of any therapy is determined by universal mechanisms: the real connection, the creation of expectations through an explanation of the disorder, and the implementation of specific functional actions. By understanding these common factors, we can make AI-powered therapy more effective and personal, which is a key part of making sure people get the help they need [17].

In response to the risks of dehumanization, the concept of Humanistically oriented artificial intelligence places human psychological needs, cognitive processes, and

ethical considerations at the core of algorithm development [18]. This includes:

- Theory of mind requires the designing AI systems that can predict human intentions and emotional states with high accuracy.
- Emotional intelligence is related to the ability of a machine to respond in a validating manner, which increases the trust of users in emotionally sensitive situations.
- Existential support requires the use of AI to facilitate meaning-centred dialogue and assist the individual in constructing personal values [19].

As these models continue to develop, it's clear that AI has the potential to enhance treatment results by taking into account the unique cultural and personal expectations of each patient, ultimately leading to more effective and personalized care [17].

D. Ethical and legal imperatives of the introduction of digital and AI-driven solutions in mental healthcare

The rapid penetration of AI in sensitive areas such as mental health requires strict regulation. The European Union Artificial Intelligence Act (EU AI Act), finally adopted in 2024, establishes the world's first comprehensive risk-based legal framework [20].

According to Article 5 of the Act, certain applications of AI in healthcare are explicitly prohibited due to unacceptable risks to fundamental rights:

- cognitive manipulation - systems that use subliminal techniques to change the behaviour of vulnerable groups;
- social scoring - classification of citizens based on behaviour or personal characteristics, which could limit access to healthcare;
- exploitation of vulnerabilities - algorithms that take advantage of the age, disability or economic situation of patients.

Most AI systems used for diagnosis and treatment in therapy are classified as "high-risk" and must meet strict requirements for transparency, traceability and mandatory human oversight. Human oversight is critical to prevent the tendency for clinicians to blindly trust the output of an algorithm, referred to as "automation bias".

Ethical challenges in AI also involve dealing with biased data. If AI is trained on unrepresentative samples, it can lead to systematic errors in diagnosing women or minority groups [21]. Privacy and data security is another important aspect, because medical information is extremely sensitive, so it needs to be strongly protected with good encryption and by following the HIPAA and GDPR standards [22].

E. Integration of Bulgaria into the European digital space and legal imperatives of the remote medical care

Bulgaria is actively integrating into the European digital space through programs such as "Digital Bulgaria 2025", National strategy for digital transformation 2020-

2030, National health strategy 2030 and the National Strategy for e-Health and Digitalization of the Health System 2030 [23] – [26]. The priorities of the Bulgarian strategy are accompanied by specific measures and directed to different target groups (Table 3). The Ministry of Health has developed a vision for AI implementation that emphasizes supporting clinicians and improving the efficiency of hospital processes. Mental healthcare is part of the broader digital health and remote medical care framework.

According to Art. 6b of the Law on Medical Institutions medical institutions and medical specialists may provide remote medical care, which includes diagnostic, treatment, rehabilitation and preventive activities and is provided in compliance with the medical standards, by applying methods approved by medical science and practice and through medical, information and communication technologies that guarantee the security of personal data and health information [27]. Remote medical assistance is provided after informed consent has been expressed by the patient in accordance with Article 87 of the Health Act.

The Ministry of Health has finalized the first comprehensive Regulation on remote medical care. It is aimed at introducing innovative and secure digital solutions in healthcare in Bulgaria, creating a modern regulatory framework [28].

The regulatory act was developed in connection with the amendments to the Law on Medical Institutions and aims to introduce clear rules for diagnostics, treatment, prevention and monitoring of patients through telemedicine services.

Remote medical care will be provided by medical institutions and medical specialists in compliance with all established standards and rules for good medical practice. Telemedicine will be applied only in cases where the same level of quality and safety of medical care can be guaranteed as is provided in face-to-face healthcare.

TABLE 3 BULGARIAN INTEGRATION OF THE EUROPEAN DIGITAL SPACE

Priority of the Bulgarian strategy	Measures and target groups	
	Specific measures	Target group
Digital skills	Training programs for rebalancing competences	Young people (16-24 years) and adults
E-health	Expanding access to services through digital channels	Population in remote regions
Prevention and diagnostics	Implementing AI in medical imaging and screening	Patients with chronic and brain diseases
Ethical standards	Creating a framework for protecting patients' rights	All users of AI services
Integrated care	Digitalization of the psychiatry-social services link	People with severe mental disorders

Particular emphasis is placed on the protection of personal data, the security of health information and the traceability of medical activities. All telemedicine services performed will be documented in the patient's electronic health record through the National Health Information System. This guarantees transparency, continuity of care and better coordination between medical specialists. The regulation creates conditions for more accessible, timely and modern healthcare, enabling more patients to receive quality medical care regardless of their location.

Nevertheless, the Regulation on remote medical care should be more detailed in regard to object, stakeholders and exceptions. The texts should be refined to ensure both a high level of patient protection and the real applicability of telemedicine in everyday medical practice. The sensitive medical data storage is another problematic issue that should be regulated more clearly in order to guarantee privacy and security.

Concerning the AI-driven solutions in medical care, surveys among Bulgarian specialists (e.g. ophthalmologists and neurologists) show "cautious optimism." [29]. While younger clinicians are more informed and open to new technologies, the overall level of trust in AI for making definitive diagnoses remains moderate.

Despite ambitious plans, Bulgaria faces challenges such as staff shortages, regional disparities and the need to further develop scientific infrastructure. Overcoming stigma and investing in outpatient care are emerging as long-term priorities.

F. Future perspectives

There is a demand-supply gap in mental health care, evident from the long waiting lists, health inequalities and access to care, treatment and support. The reason is the growing number of people seeking mental health and the shortage of mental health specialists, hindering expansion and reform, leaving services in a state of constant crisis.

There is also a growing necessity for measures and investment in the field of prevention and early intervention in order to preserve and enhance the society wellbeing.

The pandemic has demonstrated the role that digital technologies can play in supporting institutions, services, systems and individuals to meet the challenges they face. The knowledge and experience gained can be built upon, including the opportunity to expand the research and evidence base, develop key protocols, evaluation processes and regulation.

The mental health care landscape is changing rapidly, with digital solutions playing an increasingly important role. Multiple factors are driving this change, including the increased demand for accessible and convenient mental health support.

Digital solutions are evolving to meet this demand. A growing body of research shows that digital solutions for mental health can be as effective as traditional face-to-face therapies, often providing additional benefits such as increased accessibility and convenience. The flexibility and

anonymity offered by digital platforms often allow people to seek help that they would not otherwise have done.

One of the most significant benefits of digital solutions is their ability to make mental health support more accessible. For many people, traditional therapy may be out of reach due to various barriers, such as geographic location, cost, and existing societal stigma. Digital solutions can help overcome these obstacles by providing support to those who need it most.

There is an increasing uptake of digital tools in mental health care. Various companies are planning to focus on communication, resilience, and emotional intelligence.

When choosing a digital mental health solution, users should be guided by the features it provides, such as easy and consistent access, connection to a therapist, clinical proven effectiveness, personalized content, real-time user information, good design, etc.

Paradoxically, while helping with treatment, AI can also be a source of mental health problems. The concept of AI-induced technostress describes the negative psychological effects of automation on employees, including anxiety about job insecurity, cognitive overload, and a sense of lack of control. Long-term exposure to a work environment dominated by algorithms is associated with emotional exhaustion and depressive symptoms. This highlights the need for a balanced approach in which technological integration is accompanied by measures to support the well-being of users and professionals themselves.

In order to overcome the challenges of the introduction and use of digital solutions in mental health care, it is necessary to create the appropriate regulatory framework, conduct clinical studies and provide validation evidence. Issues related to security and privacy should be addressed by regulatory and technological means. Sensitive data protection is crucial, especially in cross border interactions, in terms of national security defence.

Clinical validation to demonstrate efficacy is a well-established and standardized process and is considered vital in the healthcare sector. Clinical studies are time-consuming, expensive and the proposed solution undergoes a rigorous validation process.

The purpose of clinical validation is to ensure that the digital solution is safe, works for all demographic segments and the results are compared to established standards. The conclusions are usually published and available for peer review. Clinically validated digital mental health solutions are based on the principle of "first, do no harm".

An analysis published in JMIR Mental Health found that only 3.4% of apps offering therapeutic treatment for anxiety and depression have published any evidence of efficacy [30]. The ability to identify applications and services that truly offer effective solutions is a key challenge facing consumers today.

The transformation of mental health care can be successfully managed by offering quality, effective and personalized digital mental health solutions that are

supported by clinical research and evidence and build trust with consumers. Such solutions should be easy to use and allow for integration with other systems. All of this should be accompanied by the creation of an ecosystem that engages stakeholders and offers a complete solution for mental health care.

IV. CONCLUSION

In conclusion, we could say that digital solutions will continue to play a key role in mental health care. As technology continues to evolve, we can expect these solutions to become even more sophisticated, offering improved support and better outcomes for people.

Artificial intelligence is in the process of fundamentally redefining mental health care, moving from the phase of theoretical potential to large-scale clinical implementation. The analysis of current trends and research allows the formulation of certain conclusions. AI provides tools for objectifying psychiatric diagnoses through multimodal biomarkers, which lays the foundations for personalized medicine and represents a diagnostic revolution.

In regard to the therapeutic efficacy, digital conversational agents have been proven effective in mild to moderate anxiety and depression, offering non-inferior results to traditional methods with significantly lower resources.

Successful integration requires strict compliance with regulations such as the EU AI Act, ensuring that AI remains a tool in the hands of a human, not an autonomous decision-making entity. As far as Bulgaria is concerned, the country has a strategic framework, but needs to accelerate the development of digital literacy and ensure a fair distribution of technological benefits between regions. The model of human-machine collaboration is the most promising way forward, providing both scalability and a deeply humane approach.

AI should not be perceived as competition for human therapy, but as its most powerful ally. By combining the algorithmic power of big data with the unique human capacities for empathy and ethical judgment, society can build a more equitable, accessible, and effective mental health support system. Professional communities must embrace this shift proactively, investing in "AI literacy" and participating in the design of tools that protect the dignity and rights of patients.

Digitalisation has the potential to play a crucial role in addressing needs in a way that traditional service models cannot. Interventions and services have the potential to become more efficient, for example through electronic patient records; there is the opportunity to provide services in ways that widen access and allow for earlier interventions, and people who need care and treatment can find the support they need. To realise this potential, collaboration between policymakers, professionals and non-governmental organisations is crucial. Successful implementation will also rely on involvement and interaction with individuals who use mental health services, as well as society as a whole.

ACKNOWLEDGMENTS

The article has been made possible with the financial support of Project No NID 44/30.03.2026 by UTP –Sofia.

REFERENCES

- [1] B. Schmeisser, T. Saebi, A.P.J. Schotter and P. Gooderham, The digital transformation of international business: A conceptualization, multidisciplinary review, and research agenda, *Journal of World Business*, Volume 61, Issue 1, 2026. <https://doi.org/10.1016/j.jwb.2025.101695>.
- [2] WHO. World Mental Health Day: an opportunity to kick-start a massive scale-up in investment in mental health. 2020 [online]. Available: <https://www.who.int/news> [Accessed Feb 11, 2026].
- [3] D. Liñan. Mental health in the "era" of artificial intelligence: technostress and the perceived impact on anxiety and depressive disorders-an SEM analysis. *Front Psychol*. 2025 Jun 2;16:1600013. <https://doi.org/10.3389/fpsyg.2025.1600013>. PMID: 40524827; PMCID: PMC12169247.
- [4] A. Hatch, J. Hoffman, R. Ross and J. Docherty. Expert Consensus Survey on Digital Health Tools for Patients With Serious Mental Illness: Optimizing for User Characteristics and User Support. *JMIR Ment Health*. 2018. e46.
- [5] E. Stratton, A. Lampit, I. Choi, R. Calvo, S. Harvey and N. Glozier. Effectiveness of eHealth interventions for reducing mental health conditions in employees: A systematic review and meta-analysis. *PLOS One*. 2017.
- [6] P. Cuijpers, A. Beekman and C. Reynolds. 3rd Preventing depression: a global priority. *JAMA* 10331034. 2012.
- [7] D. Mohr, M. Burns, St. Schueller, Gr. Clarke and M. Klinkman. Behavioral Intervention Technologies: Evidence review and recommendations for future research. *Gen Hosp Psychiatry*. 2010. 332–338.
- [8] M. Ali, S. Ali, Q. Abbas, Z. Abbas and S. W. Lee. Artificial intelligence for mental health: A narrative review of applications, challenges, and future directions in digital health. *Digit Health*. 2025 Nov 17;11:20552076251395548. <https://doi.org/10.1177/20552076251395548>. PMID: 41262770; PMCID: PMC12623648.
- [9] İ. Baydili, B. Tasci and G. Tasci. Artificial Intelligence in Psychiatry: A Review of Biological and Behavioral Data Analyses. *Diagnostics (Basel)*. 2025 Feb 11;15(4):434. <https://doi.org/10.3390/diagnostics15040434>. PMID: 40002587; PMCID: PMC11854694.
- [10] L. Liu, Z. Li, Y. Hu, C. Li, S. He, S. Zhang, J. Gao, H. Zhu and G. Huang. Predictive Performance of Machine Learning for Suicide in Adolescents: Systematic Review and Meta-Analysis. *J Med Internet Res*. 2025 Jun 16;27:e73052. <https://doi.org/10.2196/73052>. PMID: 40522723; PMCID: PMC12209725.
- [11] L. Hummel, K. C. Lorenz-Artz, J. J. Bierbooms and I. M. Bongers. Developing a Suicide Risk Prediction Algorithm Using Electronic Health Record Data in Mental Health Care: Real-World Case Study. *JMIR Med Inform*. 2026 Jan 14;14:e74240. <https://doi.org/10.2196/74240>. PMID: 41534082; PMCID: PMC12803502.
- [12] K. J. Krause, S. E. Davis, Z. Yin, K. M. Schafer, S. T. Rosenbloom and C. G. Walsh. Enhancing Suicide Attempt Risk Prediction Models with Temporal Clinical Note Features. *Appl Clin Inform*. 2024 Oct;15(5):1107-1120. <https://doi.org/10.1055/a-2411-5796>. Epub 2024 Sep 9. PMID: 39251213; PMCID: PMC11655152.
- [13] C. Palmer, E. Marshall, E. Millgate, G. Warren, M. Ewbank, E. Cooper, S. Lawes, A. Smith, C. Hutchins-Joss, J. Young, M. Bouazzaoui, M. Margoum, S. Healey, L. Marshall, S. Mehew, R. Cummins, V. Tablan, A. Catarino, A. Welchman and A. Blackwell. Combining Artificial Intelligence and Human Support in Mental Health: Digital Intervention With Comparable

- Effectiveness to Human-Delivered Care. *J Med Internet Res* 2025;27:e69351. URL: <https://www.jmir.org/2025/1/e69351>. <https://doi.org/10.2196/69351>.
- [14] R. Lederman and S. D'Alfonso. The Digital Therapeutic Alliance: Prospects and Considerations. *JMIR Ment Health*. 2021 Jul 20;8(7):e31385. <https://doi.org/10.2196/31385>. PMID: 34283035; PMCID: PMC8335609.
- [15] A. Malouin-Lachance, J. Capolupo, C. Laplante and A. Hudon. Does the Digital Therapeutic Alliance Exist? Integrative Review. *JMIR Ment Health* 2025;12:e69294. URL: <https://mental.jmir.org/2025/1/e69294>. <https://doi.org/10.2196/69294>.
- [16] X. Dai, L.L. Leng, Y. Liu, Y. T. Huang and D. F. K. Wong. The paradox of agency in psychotherapy: How people with mental distress experience support from generative AI chatbots and human therapists. *BMC Psychiatry*. 2025 Dec 12;26(1):49. <https://doi.org/10.1186/s12888-025-07671-w>. PMID: 41382092; PMCID: PMC12817506.
- [17] O. Giotakos. Artificial intelligence-based psychotherapy: focusing on common psychotherapeutic factors. *Front Psychiatry*. 2025 Nov 11;16:1710715. <https://doi.org/10.3389/fpsy.2025.1710715>. PMID: 41306320; PMCID: PMC12645830.
- [18] M. T. Khan. Integrating Psychological Theories into AI Design: A Narrative Review of Human-Centred Artificial Intelligence (HCAI). *Psychology*, 16, 1084-1095. 2025.
- [19] E. Mitsea, A. Drigas and C. Skianis. Systematic Review of Artificial Intelligence in Positive and Existential Psychiatry: Advancing Mental and Emotional Health Through Metacompetency Development. *Healthcare*. 2026; 14(6):783. <https://doi.org/10.3390/healthcare14060783>.
- [20] Artificial Intelligence Act [online]. Available: <https://ai-act-law.eu/> [Accessed Feb 10, 2026].
- [21] T. Tavory. Regulating AI in Mental Health: Ethics of Care Perspective. *JMIR Ment Health*. 2024 Sep 19;11:e58493. <https://doi.org/10.2196/58493>. PMID: 39298759; PMCID: PMC11450345.
- [22] H. R. Saeidnia, S. G. Hashemi Fotami, B. Lund and N. Ghiasi. Ethical Considerations in Artificial Intelligence Interventions for Mental Health and Well-Being: Ensuring Responsible Implementation and Impact. *Social Sciences*. 2024; 13(7):381. <https://doi.org/10.3390/socsci13070381>.
- [23] National program "Digital Bulgaria 2025" [online]. Available: <https://www.mtc.government.bg> [Accessed Feb 11, 2026].
- [24] National strategy for Digital transformation 2020-2030 [online]. Available: <https://digitalalliance.bg/strategy-digital-transformation-bulgaria/> [Accessed Feb 12, 2026].
- [25] National health strategy 2030 [online]. Available: <https://old.mh.government.bg/bg/politiki/strategii-i-kontseptsii/strategii/nacionalna-zdravna-strategiya-2030/> [Accessed Feb 13, 2026].
- [26] National Strategy for e-Health and Digitalization of the Health System 2030 [online]. Available: <https://old.mh.government.bg/bg/politiki/strategii-i-kontseptsii/strategii/nacionalna-strategiya-za-elektronno-zdraveopazvane-i-digitalizac/> [Accessed Feb 14, 2026].
- [27] Law on Medical Institutions [online]. Available: <https://www.parliament.bg/bg/desision/ID/165756> [Accessed April 14, 2026].
- [28] Regulation on remote medical care [online] Available: <https://www.mh.government.bg/bg/normativni-aktove/proekti-na-normativni-aktove/70> [Accessed April 25, 2026].
- [29] M. N. Radeva, E. Hristova, R. T. Georgiev and Z. I. Zlatarova. Awareness, trust, and expectations of AI for glaucoma care among Bulgarian ophthalmologists: Role of demographic factors. *PLOS Digit Health*. 2026 Jan 22;5(1):e0001199. <https://doi.org/10.1371/journal.pdig.0001199>. PMID: 41569993; PMCID: PMC12826508.
- [30] J. M. Marshall, D. A. Dunstan and W. Bartik. Apps With Maps—Anxiety and Depression Mobile Apps With Evidence-Based Frameworks: Systematic Search of Major App Stores. *JMIR Ment Health* 2020;7(6): e16525. <https://doi.org/10.2196/16525>.

Water Resources Exploitation in Bulgaria: A Water Security Perspective

Desislava Dimitrova

dept. Ecology and Environmental
Protection, Shipbuilding Faculty Technical University
Varna, Bulgaria
ORCID 0009-0005-4962-3430

Daniela Toneva

dept. Ecology and Environmental Protection, Shipbuilding
Faculty
Technical University
Varna, Bulgaria
ORCID [0000-0003-1599-395X](https://orcid.org/0000-0003-1599-395X)

Abstract— This study examines the exploitation of water resources in Bulgaria within the framework of water security, with particular emphasis on the structural transformation of water supply systems and the increasing strategic role of groundwater. The analysis is based on River Basin Management Plans (2022–2027), national statistical data, and a comprehensive assessment of water abstraction dynamics across the four river basin districts for the period 2010–2024. The results reveal a clear shift from surface water dominance towards a groundwater-driven supply model, characterized by a decline in surface water abstraction from 488.3 million m³ in 2010 to 386.1 million m³ in 2024, and a relatively stable but increasingly dominant role of groundwater, which accounts for over 50% of total public water abstraction on average and reaches approximately 78–81% of drinking water supply at national level. The findings demonstrate that, despite the existence of significant reservoir infrastructure, the long-term stability and resilience of water supply in Bulgaria are predominantly sustained by groundwater resources, which function as a buffering and stabilizing component of the system.

Keywords—groundwater, water management, water resources, water security

I. INTRODUCTION

Water resources constitute a fundamental component of natural capital and a key determinant of socio-economic development and stability, supporting ecological balance [1]. At the same time, maintaining water resource quality and quantity is considered a matter of national security in every country. Under conditions of accelerating climate change, intensifying urbanization, and increasing resource demand, water management is evolving from a traditional sectoral activity into a strategic instrument for ensuring water security [2], [3].

Water security is a complex and multidimensional concept that encompasses the capacity of a system to

ensure sustainable, reliable, and sufficient access to water resources of appropriate quality to meet the needs of the population, the economy, and ecosystems, while simultaneously minimizing risks associated with water scarcity, pollution, and extreme hydrological events [4], [5], [22]. It includes both the quantitative and qualitative management of water resources, as well as effective risk management, sustainable resource use, and adaptation to climate variability [6], [17], [21]. In a contemporary context, water security is increasingly recognized as a key component of national security and sustainable development, closely interconnected with energy and food security, as well as environmental protection.

In Bulgaria, water resources are characterized by relatively limited availability and pronounced spatial and seasonal variability [7]. The long-term average annual runoff amounts to approximately 21.3 km³/year, while a significant share of the available water resources is generated outside the national territory in the form of transboundary inflow, resulting in dependence on external hydrological systems and increased vulnerability to climatic and anthropogenic factors [8], [9].

Furthermore, climate variability has led to an increased frequency and intensity of extreme events, such as droughts and floods, which directly affect both the quantity and quality of water resources [10], [21].

At the same time, different river basin districts exhibit distinct hydrological characteristics and temporal dynamics, reflecting variations in resource availability, water use patterns, and socio-economic pressures.

In Bulgaria, groundwater resources are represented by more than 170 groundwater bodies and play a strategic role in securing drinking water supply for the population. According to national statistical data (NSI), groundwater accounts for a dominant share in public water supply, reaching approximately 78–81% during the period 2014–

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.128>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

2020 [11]. This confirms its critical importance as the primary source for drinking water supply at the national level, with even higher dependence observed in certain regions. Consequently, groundwater constitutes a key pillar of water security in Bulgaria. At the same time, groundwater vulnerability to overexploitation and contamination necessitates the adoption of sustainability-oriented and scientifically grounded management approaches [12], [24].

The exploitation of water resources in Bulgaria exhibits a clearly defined sectoral structure, including public water supply, agriculture (irrigation), industrial use, and energy production. Total annual water abstraction ranges between 5.5 and 6.5 billion m³, with the energy sector accounting for the largest share (60%), followed by agriculture (20–25%), industry (10–15%), and domestic water supply (10%). Despite its relatively smaller share, drinking water supply is of critical importance for water security, as it is directly linked to public health and quality of life [4], [7].

The analysis of water abstraction across river basin districts reveals substantial regional disparities. The Danube Basin District is characterized by relatively good water availability and a dominant reliance on groundwater resources. In contrast, the East Aegean Basin District exhibits the highest level of water use (approximately 2.5 billion m³/year) and a significant dependence on reservoir systems, making it particularly vulnerable to drought conditions. Although drone-based observations are promising, they are not yet widely implemented in the monitoring of available water resources in Bulgaria [14], [15].

The Black Sea Basin District is subject to strong seasonal pressure driven by tourism, while the West Aegean Basin District has more limited water resources and relies heavily on groundwater and transboundary river systems.

Despite the available resource potential, the efficiency of water use in Bulgaria remains a significant challenge. Total water losses in the water supply and sewerage sector are estimated at approximately 1102 million m³ per year on average, accounting for about 56.8% of the total water supplied nationwide over the period 2010–2023. These losses are primarily attributed to the deteriorated water supply infrastructure and system failures, and are largely classified as real (physical) losses. This constitutes a major structural weakness of the water sector, necessitating a transformation of existing management models [3], [12], [23].

In this context, the present study aims to analyze the water use in Bulgaria through the lens of water security, with a focus on quantitative parameters of water use, regional disparities, and the role of groundwater as a strategic resource.

II. MATERIALS AND METHODS

The analysis is based on data obtained from River Basin Management Plans, the National Statistical Institute (NSI), the Ministry of Environment and Water (MOEW), and the Executive Environment Agency (EEA) [2], [7], [11]. The

study covers the period 2010–2024 and includes all four river basin districts in Bulgaria: Danube, Black Sea, East Aegean, and West Aegean River Basin Districts - reflecting the country's natural hydrographic structure. Based on their territorial extent, calculated from basin area distribution (Danube – 49,950 km²; East Aegean – 47,730 km²; Black Sea – 13,320 km²; West Aegean – 13,500 km²), the Danube Basin accounts for approximately 48% of the national territory, followed by the East Aegean - 35%, the Black Sea-10%, and the West Aegean - 7%, highlighting significant spatial disparities in water resource distribution [16]. The methodological approach combines comparative statistical analysis, trend analysis, and interpretation of quantitative indicators related to water abstraction, groundwater use, public water supply, and water losses. The analysis was conducted using officially reported annual data expressed in million m³/year and percentage shares (%). Comparative assessment between river basin districts was performed in order to identify regional disparities, dominant water sources, and water security vulnerabilities.



Fig. 1. Spatial distribution of river basin districts in Bulgaria.

The spatial distribution of the population was incorporated as a key factor influencing pressure on water resources [8], [12]. Additionally, an assessment of water-use efficiency was performed, alongside the identification of principal risks associated with climate variability and water stress [3].

The analyses were conducted within the broader framework of assessing water security and sustainable water resource management in Bulgaria.

III. RESULTS AND DISCUSSION

Water resource management is directly related to the security and resilience of critical infrastructure systems. In the context of climate change and increasing environmental pressures, water security is becoming an essential component of national and regional security policies.

In accordance with the current regulatory framework, including the Water Act, the Water Framework Directive (2000/60/EC), and Decree No. 181/2009 on the designation of strategic sites of national security importance, water bodies in Bulgaria are classified into two main categories—surface water and groundwater [13], [18], [19], [20]. Surface waters comprise an extensive river network exceeding 20,000 km in length, as well as a substantial

number of artificial water bodies, including more than 2,000 reservoirs.

A key component of Bulgaria's water security is represented by the 52 complex and significant reservoirs, among which those designated as nationally important for drinking water supply play a particularly strategic role [20], Table 1.

The stored volumes allocated for drinking water supply account for 83.68% of their total capacity, underscoring their critical function in maintaining the resilience and reliability of the national water supply system [10].

Within the Danube River Basin District, the reservoirs Iskar, Ogosta, Srechenska Bara, Yovkovtsi, and Beli Iskar play a central role in supplying water to large parts of Northern and Western Bulgaria, including the capital city of Sofia. In particular, Iskar Reservoir, with a storage capacity of approximately 673 million m³, provides nearly two-thirds of Sofia's drinking water demand.

TABLE 1

KEY RESERVOIRS OF NATIONAL IMPORTANCE FOR DRINKING WATER
 SUPPLY ACROSS RIVER BASIN DISTRICTS IN BULGARIA

Reservoir	Key Characteristics			
	River Basin District	Total Storage Capacity (million m ³)	Primary Use	Population Served (approx)
Iskar	Danube RBD	520	Drinking water supply, energy	1.5–2.0 million (Sofia)
Ogosta	Danube RBD	506	Irrigation, water supply	150,000
Yovkovtsi	Danube RBD	92.18	Drinking water supply	120,000 (Veliko Tarnovo)
Srechenska Bara	Danube RBD	15.50	Drinking water supply	80,000
Beli Iskar	Danube RBD	15.45	Drinking water supply	70,000
Kardzhali	East Aegean RBD	497	Energy, water supply	100,000
Studena	East Aegean RBD	25	Drinking water supply	100,000 (Pernik)
Ivaylovgrad	East Aegean RBD	188	Energy, water supply	50,000
Asenovets	East Aegean RBD	28	Drinking water supply	60,000 (Sliven)
Batak	East Aegean RBD	310	Energy, water supply	80,000
Arda	East Aegean RBD	1077.9	Energy, water supply	100,000

Reservoir	Key Characteristics			
	River Basin District	Total Storage Capacity (million m ³)	Primary Use	Population Served (approx)
Ticha	East Aegean RBD	149	Drinking water supply	200,000 (Shumen, Targovishte)
Kamchiya	Black Sea RBD	110	Drinking water supply	500,000 (Varna, Burgas)
Yasna Polyana	Black Sea RBD	35.3	Drinking water supply	250,000 (Southern Black Sea coast)
Tsonevo	Black Sea RBD	109	Water supply, irrigation	100,000
Pancharevo	West Aegean RBD	6.7	Regulation, water supply	Local significance
Hristo Smirnenki	West Aegean RBD	31	Drinking water supply	50,000
Borovitsa	West Aegean RBD	27.3	Drinking water supply	Local significance

In the East Aegean River Basin District, reservoirs such as Kardzhali, Studena, Ivaylovgrad, Asenovets, Batak, Arda, and Ticha are of strategic importance, serving both water supply and the energy and irrigation sectors. The Black Sea River Basin District includes reservoirs such as Kamchiya, Yasna Polyana, and Tsonevo, which are primary sources of drinking water for coastal and tourist regions characterized by pronounced seasonal water stress.

In the West Aegean River Basin District, reservoirs such as Pancharevo, Hristo Smirnenki, and Borovitsa play an important regional role in securing water resources under conditions of limited natural availability.

Despite the key role of nationally significant reservoirs in ensuring drinking water supply, the analysis of the water supply structure in Bulgaria indicates that surface water does not constitute the dominant source at the national level. Its exploitation is highly dependent on climate variability, seasonal fluctuations in runoff, and reservoir storage levels, which limits its reliability as a sustainable resource under drought conditions.

In this context, groundwater emerges as the primary strategic source for public water supply, providing between 65% and 70% of total water supply nationwide, with shares exceeding 70% in certain regions [11]. This dependence is particularly pronounced in areas with limited surface water availability or high seasonal demand, where groundwater bodies function as a buffering system, compensating for deficits in surface water resources.

A comparative assessment of reservoir systems and groundwater highlights a clear functional differentiation

within the water supply system [8]. While reservoirs provide substantial water volumes and play a critical role in regulating water resources and meeting peak demand, groundwater ensures long-term stability, continuity, and reliability of water supply.

An analysis of data for the period 2010–2024 reveals a pronounced structural transformation in the composition of water used for public water supply in Bulgaria (Fig. 2).

The most significant trend is the gradual decline in the use of surface water, accompanied by a corresponding increase in groundwater abstraction, indicating a clear shift from surface to groundwater sources for public water supply and sewerage.

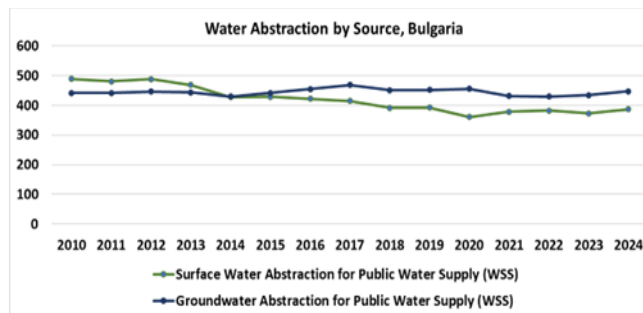


Fig. 2. Surface and Groundwater Abstraction for Public Water Supply in Bulgaria (2010–2024)

*WSS = Water Supply and Sewerage

At the beginning of the analyzed period, surface water dominated the total volume of water abstraction for public water supply, reaching 488.318 million m³ in 2010, compared to 441.094 million m³ of groundwater. However, by the end of the period, a clear restructuring of this relationship is observed. In 2024, surface water abstraction decreased to 386.12 million m³, while groundwater abstraction increased to 447.24 million m³.

Additional significance lies in the change in the relative share of the two water sources. In 2010, groundwater accounted for approximately 47.5% of the total water abstraction for public supply, whereas by 2024 its share had increased to around 53.7%. On average, groundwater constituted about 51.6% of the total water supply for drinking purposes over the entire period. This dynamic confirms the growing dependence of the water supply sector on groundwater resources.

The analysis of water abstraction dynamics for public water supply over the period 2010–2024 further reveals pronounced spatial and temporal differences among the four river basin districts in Bulgaria (Fig. 3).

The largest share of total water supply is attributed to the Danube River Basin District, where values range between 169.8 and 188.8 million m³/year. The maximum is observed in 2013 (188.8 million m³), followed by a gradual decline until 2021 and a slight recovery by 2024 (178.99 million m³). This trend can be interpreted as the result of a combined influence of demographic factors, improvements in water use efficiency, and climatic variability.

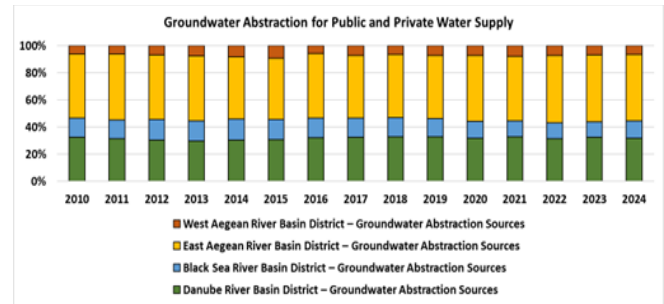


Fig. 3. Groundwater Abstraction by River Basin Districts in Bulgaria (2010–2024)

The East Aegean River Basin District ranks second in terms of water use, with values ranging between 87.5 and 101.9 million m³/year. A relatively stable trend is observed, with a slight increase during the period 2015–2017, when a peak of approximately 101.9 million m³ is reached, followed by stabilization around 95–100 million m³. This reflects sustained demand for water resources in a region characterized by high economic activity and a significant agricultural sector.

The Black Sea River Basin District exhibits the highest variability, with water use increasing from 65.5 million m³ in 2010 to a peak of 96.9 million m³ in 2020, followed by a sharp decline in 2021 (68.5 million m³) and a gradual recovery thereafter. This dynamic is directly related to the seasonal nature of water demand driven by tourism, as well as to external factors such as climatic conditions and socio-economic fluctuations.

The West Aegean River Basin District is characterized by the lowest and relatively stable values, ranging between 29.08 and 32.5 million m³/year, reflecting both limited water resources and lower levels of urbanization and industrial development in the region.

The analysis of groundwater abstraction for public and self water supply across river basin districts reveals a pronounced spatial asymmetry. The East Aegean River Basin District plays a dominant role, consistently accounting for the largest share of total groundwater abstraction throughout the analyzed period. Quantitative data indicate that groundwater abstraction in this district ranges between 251.695 and 274.427 million m³/year, with an average annual value of approximately 264.9 million m³. Its relative share in national groundwater use is estimated at approximately 46–50%. The district encompasses major urbanized areas and industrial centers, which generate high demand for water resources.

The Danube River Basin District ranks second in terms of groundwater abstraction, with values ranging between 166.418 and 187.865 million m³/year and an average of approximately 177.5 million m³. Despite its significant contribution to national water supply, its share remains noticeably lower than that of the East Aegean District.

The Black Sea River Basin District occupies the third position, with groundwater abstraction ranging between 62.228 and 84.366 million m³/year and an average of approximately 76.4 million m³. This district is characterized by higher variability, likely associated with

seasonal pressures on water supply systems due to tourism and concentrated demand in coastal areas. A declining trend is observed after 2020, followed by partial recovery in 2024, indicating sensitivity to changing economic and climatic conditions.

The lowest values are observed in the West Aegean River Basin District, where groundwater abstraction remains within the range of 33.033–51.677 million m³/year, with an average of approximately 39.3 million m³. Although its share in national groundwater abstraction is limited, its regional importance remains significant, particularly given the reliance on groundwater sources in areas with constrained water availability.

The analysis of water use for public water supply across the river basin districts in Bulgaria for the period 2010–2024 reveals pronounced spatial and temporal disparities, reflecting both the natural characteristics of water resources and the socio-economic factors driving water consumption (Fig. 4).

The Danube River Basin District consistently accounts for the largest share throughout the analyzed period, with values ranging approximately between 170 and 190 million m³/year. A relatively stable trend is observed, with a slight decline during the period 2018–2021, followed by a recovery towards the end of the period.

The East Aegean River Basin District ranks second, with values ranging between 90 and 102 million m³/year. The trend is characterized by moderate variability, with a distinct peak observed around 2016–2018, followed by a stabilization phase.

The Black Sea River Basin District exhibits the highest degree of variability and dynamic change. Water use increases from approximately 65 million m³ in 2010 to a peak of around 95–100 million m³ during the period 2018–2020, followed by a sharp decline in 2021 and partial recovery in subsequent years.

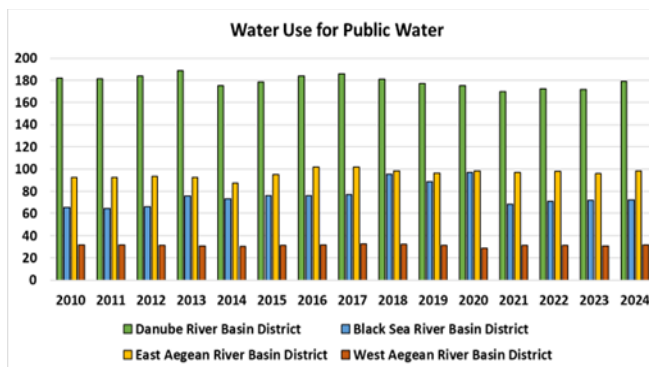


Fig. 4. Regional distribution of water use for public water supply in Bulgaria by river basin districts (2010–2024).

The West Aegean River Basin District is characterized by the lowest and relatively stable values, ranging between 28 and 33 million m³/year.

The East Aegean River Basin District is thus established not only as the region with the highest groundwater abstraction but also as the most vulnerable in

terms of risks related to overexploitation, declining groundwater levels, and deterioration of chemical status. The district includes seven reservoirs designated as strategic objects of national security importance—Kardzhali, Studena, Ivaylovgrad, Asenovets, Batak, Arda, and Ticha—which further reinforces its significance within the national water management system. The combination of high groundwater abstraction and the concentration of key water infrastructure underscores the critical role of the East Aegean District and highlights its strategic importance for ensuring water security in Bulgaria. In this context, the sustainable management of groundwater bodies—including control of abstraction, monitoring of quantitative and chemical status, and mitigation of anthropogenic pressures—represents a key priority in national water policy.

In the context of increasing climate variability, intensifying anthropogenic pressure, and structural imbalances in water use, the future management of water resources in Bulgaria is defined by the need to transition toward an integrated and adaptive management framework. The growing role of groundwater as a strategic resource for ensuring long-term water security is becoming increasingly evident, necessitating the implementation of stricter monitoring regimes, enhanced control over water abstraction, and effective protection of water quality. At the same time, the modernization of water supply infrastructure and the reduction of losses within water supply and sewerage networks represent key priorities for improving the efficiency of water use.

Regional disparities in the availability and consumption of water resources require the application of differentiated management approaches tailored to the specific hydrological and socio-economic characteristics of individual river basin districts. Particular attention should be given to the East Aegean River Basin District, where the high concentration of water abstraction and strategic infrastructure increases the risk of overexploitation and resource degradation.

IV. CONCLUSIONS

The present study identifies a clear structural transformation in Bulgaria's water supply model, characterized by a gradual transition from the dominance of surface water resources to an increasing reliance on groundwater. In this context, groundwater emerges as a primary strategic component of the water supply system, long ensuring -term stability, reliability, and resilience under conditions of growing climatic uncertainty. Although surface waters and reservoir infrastructure continue to play a significant role, their effectiveness is increasingly constrained by their high sensitivity to seasonal variability and climate change.

The analysis of the 2010–2024 period reveals a pronounced spatial differentiation in water use patterns, with the East Aegean River Basin District clearly dominating in terms of groundwater abstraction, accounting for approximately 46–50% of the total national groundwater use. The combination of intensive

groundwater exploitation and the concentration of seven strategically significant reservoirs defines the region as a critical node within the national water security system, while simultaneously increasing its vulnerability to overexploitation, declining groundwater levels, and deterioration of chemical status.

At the regional scale, distinct hydrological and management characteristics are observed across the river basin districts. The Danube River Basin District demonstrates relatively stable water availability and resource security; the Black Sea River Basin District is characterized by high seasonal variability driven by tourism-related pressures; and the West Aegean River Basin District exhibits limited water resources and strong dependence on local groundwater sources. This heterogeneity necessitates the implementation of region-specific, adaptive water management strategies tailored to the unique hydrological and socio-economic conditions of each basin [1], [2].

Furthermore, the high level of water losses within the distribution network (50–60%) is identified as a major systemic vulnerability, significantly reducing water use efficiency and intensifying pressure on strategic water resources. In this regard, improving infrastructure efficiency, alongside the sustainable management of groundwater resources, constitutes a critical priority for ensuring long-term water security in Bulgaria.

The findings may support decision-making related to sustainable water resource management, monitoring systems, and long-term water security planning. Future research may focus on digital monitoring technologies, groundwater quality assessment, satellite and drone-based observations, and predictive water risk modeling.

REFERENCES

- [1] European Commission, “Ensuring groundwater quantity and quality across the EU,” 2022. [Online]. Available: <https://environment.ec.europa.eu/>. [Accessed: 18-May-2026].
- [2] Council of Ministers, “Decree No. 181/2009 on strategic sites of national security importance,” State Gazette, Bulgaria, 2009.
- [3] OECD, “Water governance in Europe,” 2022. [Online]. Available: <https://www.oecd.org/en/topics/water-governance.html>. [Accessed: 18-May-2026].
- [4] D. Toneva and D. Dimitrova, “Significance of groundwater resources for provision of water consumption in Varna district,” in Proc. 16th Int. Sci. Practical Conf. Environment. Technology. Resources, vol. 1, pp. 529–535, Jun. 2025, <http://doi.org/10.17770/etr2025vol1.8691>.
- [5] D. Toneva and D. Dimitrova, “Some aspects of the water crisis in Bulgaria,” in Proc. 15th Int. Sci. Practical Conf. Environment. Technology. Resources, vol. 1, Jun. 2024, <https://doi.org/10.17770/etr2024vol1.7972>.
- [6] E. K. Bankova, “Assessment of the measures implemented in Bulgarian legislation for protection of drinking water sources,” J. Biomed. Clin. Res., vol. 16, no. 1, pp. 44–54, 2023, <https://doi.org/10.2478/jbcr-2023-0006>.
- [7] Ministry of Environment and Water (MOEW), “River Basin Management Plans 2022–2027,” Sofia, Bulgaria, 2022. [Online]. Available: <https://www.moew.government.bg>. [Accessed: 18-May-2026].
- [8] K. Voudouris, “Groundwater governance in transboundary aquifers: A case study from Greece-Bulgaria,” Bulgarian Geological Society Review, 2019.
- [9] M. Falkenmark and J. Rockström, “The new blue and green water paradigm,” J. Water Resour. Plan. Manage., 2006.
- [10] United Nations Environment Programme (UNEP), “Water security and ecosystem services,” 2021. [Online]. Available: <https://www.unep.org>. [Accessed: 18-May-2026].
- [11] Ministry of Environment and Water (MOEW), “National Report on the State and Protection of the Environment in Bulgaria,” Sofia, Bulgaria, 2021. [Online]. Available: <https://www.moew.government.bg>. [Accessed: 18-May-2026].
- [12] UNESCO, “World Water Development Report,” 2023. [Online]. Available: <https://www.unesco.org/reports/wwdr/2023/en/download>. [Accessed: 18-May-2026].
- [13] National Statistical Institute (NSI), “Water use and water supply in Bulgaria – statistical data,” 2024. [Online]. Available: <https://www.nsi.bg>. [Accessed: 18-May-2026].
- [14] A. Atanasov and A. Bankova, “The influence of location accuracy on the estimation of crops with a budget UAV in Dobrudja,” in Proc. 2024 9th Int. Conf. on Energy Efficiency and Agricultural Engineering (EE&AE), Jul. 2024, <https://doi.org/10.1109/EEAE60309.2024.10600617>.
- [15] A. Atanasov, S. Stoyanov, A. Bankova, and I. Ivanov, “Method for obtaining NDVI from a single photo for very small areas,” in Proc. 2025 10th Int. Conf. on Energy Efficiency and Agricultural Engineering (EE&AE), Nov. 2025, <https://doi.org/10.1109/EEAE65901.2025.11273540>.
- [16] European Commission, “Water resilience and climate adaptation strategy,” 2023. [Online]. Available: <https://environment.ec.europa.eu>. [Accessed: 18-May-2026].
- [17] World Bank, “Water security and climate change adaptation,” 2020.
- [18] European Environment Agency, “Water resources across Europe — confronting water stress,” 2022. [Online]. Available: <https://www.eea.europa.eu/en/analysis/publications/water-resources-across-europe-confronting>. [Accessed: 18-May-2026].
- [19] European Commission, “Water Framework Directive (2000/60/EC),” 2021. [Online]. Available: https://environment.ec.europa.eu/topics/water/water-framework-directive_en. [Accessed: 18-May-2026].
- [20] Water Act, State Gazette, Bulgaria, latest amendments.
- [21] Republic of Bulgaria, National Climate Change Adaptation Strategy and Action Plan (Project No. P160511), World Bank, 2019. [Online]. Available: <https://www.moew.government.bg/static/media/ups/categories/attachments/Strategy%20and%20Action%20Plan%20-%20Full%20Report%20-%20%20ENd3b215dfec16a8be016bfa529bcb6936.pdf>. [Accessed: 18-May-2026].
- [22] UN-Water, “Water security: definition and global assessment,” 2021. [Online]. Available: <https://www.unwater.org/publications/un-world-water-development-report-2021>. [Accessed: 18-May-2026].
- [23] Water News Europe, “Profile of the Bulgarian water sector,” 2026. [Online]. Available: <https://www.waternewseurope.com/profile-bulgarian-water-sector/>. [Accessed: 18-May-2026].
- [24] T. Vasileva, “Assessing the quality of groundwater in Bulgaria for irrigation purposes – a spatial approach,” Geologica Balcanica, vol. 54, no. 2, pp. 43–55, 2025.
- [25] K. Gartsyanova, “Assessment of water quality as a key component in the water–energy–food nexus in Bulgaria,” Water, vol. 11, no. 3, p. 36, 2024.

An Integrated Simulation Model for Maritime Cybersecurity: A Comparative Research Analysis Approach

Ekaterina Dyankova

Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
edyankova@naval-acad.bg

Dilyana Dimitrova

Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
di.dimitrova@naval-acad.bg

Abstract—This paper presents the development of an integrated simulation model for maritime cybersecurity training, based on a comparative analysis of existing training platforms. For the purposes of the study, leading international and industrial solutions were evaluated, including Cyber-SHIP Lab, Naval Cyber Range, CDeX Maritime Cybersecurity Scenario, SeaSAFER, K-Sim, and NavSim. Through the applied comparative approach, the advantages and limitations of standalone physical and virtual training environments were identified. Based on these findings, a new, integrated hybrid model was designed that conceptually combines real ship bridge infrastructure with dynamic virtual cyberattack scenarios. It is concluded that the proposed architecture improves trainee preparation by simultaneously developing technical competencies, analytical thinking, and crew coordination in managing cyber incidents at sea.

Keywords— comparative analysis, hybrid simulators, integrated model, maritime cybersecurity, simulation training.

I. INTRODUCTION

Simulation technologies play a central role in the training of maritime professionals due to the increasing digitization and automation of the maritime industry. They provide a realistic learning environment in which trainees can practice various skills without risk to life and crew. The evolution of these technologies - from classical bridge simulators to modern platforms with augmented reality (Augmented Reality/Virtual Reality) elements - reflects the dynamic changes in maritime education and the need to update teaching approaches.

In recent years, maritime simulations have evolved to include environments focused on cybersecurity. This development is due to the growing reliance of modern ships on interconnected digital systems, including navigation, communication, and control technologies. While these

systems improve operational efficiency, they also create vulnerabilities that can be exploited through cyberattacks. As a result, simulation-based training is used increasingly to support the development of competencies related to navigation, engineering, cybersecurity awareness, decision-making, and coordinated response in critical situations.

Simulation-based training is aligned with the principles of experiential learning [1], enabling the acquisition of practical skills through active engagement, analysis of outcomes, and application of knowledge in realistic contexts. Maritime simulators are widely used for developing competencies such as vessel navigation, compliance with international regulations, engine room management, and emergency response [2]. The importance of such training is emphasized by the International Maritime Organization (IMO), which highlights the role of human factors and the need to learn from past incidents in order to improve safety practices.

Traditional full-mission simulators have been established as effective tools for procedural training and standards compliance, particularly within the framework of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) [3]. At the same time, emerging technologies based on virtual, augmented, and mixed reality are integrated into training environments, offering enhanced realism and user engagement [2]. A master's program in "Simulation Engineering" with a specialization in "Maritime Simulators" has been developed at the Nikola Vaptsarov Naval Academy in Varna, Bulgaria [4], reflecting the growing recognition of the importance of these technologies in the training of maritime specialists. These developments indicate a shift toward more immersive and adaptive maritime training environments.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.114>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Maritime cybersecurity has become a critical component of overall maritime safety. Effective training in this domain requires simulation platforms capable of integrating realistic operational conditions with dynamic cyber threat scenarios. Existing research demonstrates a variety of approaches to simulation-based training and system evaluation.

The main aim of the paper is to analyze and evaluate existing maritime simulation platforms from both technological and educational perspectives, and to propose an integrated hybrid model for maritime cybersecurity training.

II. MATERIALS AND METHODS

In order to evaluate current approaches to maritime cybersecurity training, a structured methodological framework is applied. The study is based on a comparative analysis of selected simulation platforms, using defined criteria that address both technological capabilities and educational effectiveness. The findings serve as the basis for the development of an integrated hybrid simulation model.

Comparative analyses have been applied in different maritime contexts. Time-domain simulations have been evaluated against experimental models in studies related to ship stability [5]. In the field of autonomous systems, hardware-in-the-loop simulations have been used to assess detection methods, demonstrating improved performance in integrated sensor approaches [6]. Augmented reality applications have been shown to enhance training effectiveness and user engagement, although limitations remain in representing complex technical interactions [7]. Similarly, virtual and immersive simulation environments contribute to the safe development of practical skills while maintaining a high level of interactivity [8].

Further studies have confirmed the reliability of simulation platforms through comparisons with real-world measurements [9]. In educational settings, the use of advanced simulators has been associated with improved decision-making, faster response times, and enhanced overall performance of trainees [10].

Despite these contributions, limited research has been identified that provides a comprehensive comparative analysis of simulation platforms specifically focused on maritime cybersecurity training. In particular, the integration of physical and virtual simulation environments within a unified training framework remains limited. This gap highlights the need for approaches that combine technological realism with structured pedagogical models for cybersecurity competence development.

A variety of maritime simulation solutions are offered by both industry and academia. Some focus on traditional tasks (navigation, engine room), while others are specifically focused on cybersecurity. In the field of maritime cybersecurity, significant progress has been made in the development of specialized simulators and training platforms. Shipping relies more and more on digitalized systems such as Electronic Chart Display and Information

System (ECDIS), AIS/GPS receivers, automated engine rooms, and communication networks. These systems are becoming more connected to the Internet via satellite and 4G/5G networks, making them vulnerable to cyberattacks. Breaches of electronic navigation systems or malware infections can lead to course deviation, loss of connectivity, accidents, and other consequences. To address these issues, a requirement was introduced in 2021 by the International Maritime Organization (IMO) (MSC.428(98)), mandating that cyber risks be included in safety management (ISM Code) [11].

An example of a modern maritime cybersecurity training facility is the Cyber-SHIP Lab at the University of Plymouth, United Kingdom, where the bridge and related ship systems of a modern vessel have been physically replicated. In this controlled laboratory environment, cyber vulnerabilities, exploits, and the operational consequences of attacks are studied by researchers and students [11]. The equipment includes ECDIS, AIS (Automatic Identification System), VDR (Virtual Data Recorder), radars, and communication devices, through which a realistic environment is provided for simulating and analyzing cyberattacks, as well as for developing practical tools and training programs for seafarers [11].

Similarly, a modular cyber range - the Naval Cyber Range - has been developed by the French Naval Academy (École Navale), replicating the IT/OT infrastructure of a medium-sized passenger ship (PLC (Programmable Logic Controller) controllers, AIS, GPS, radar, VDR, etc.) [12]. Training scenarios include phishing and malware attacks, as well as direct manipulation of navigation data. The platform is used as a realistic training tool for both naval personnel training and research [13].

Another such platform is the CDeX Maritime Cybersecurity Scenario, a joint project between CDeX, Shipadvisors, and the Maritime Academy Antwerp [14]. Participants are placed in a simulation of a 150-meter tanker (MV Vigilant Sailor), where leadership roles are assumed and a variety of cyberattacks are encountered, including fake emails, infected updates, and ECDIS sabotage through GPS jamming, AIS spoofing, and data modification (speed, depth, etc.) [15]. Through this type of training, skills for recognizing cyber threats, rapid response, and recovery under realistic conditions are developed.

The K-Sim system is offered by Kongsberg Maritime and includes full-scale bridge, engine, and environmental simulators. These products are used in universities, maritime academies, navies, coast guards, and shipping companies worldwide [16]. Similarly, NavSim products by Wärtsilä are widely used; their navigation simulators support training in both educational environments and VR/AR settings, as well as distributed (online) platforms compliant with international standards [17].

SeaSAFER, developed under the leadership of the Lithuanian Maritime Academy, is an online training platform in which real reports of maritime incidents and accidents are transformed into simulated scenarios. The

main advantages of the platform include ease of access, lower costs compared to traditional simulators, and the possibility of certification recognized in partner countries and across Europe [18].

The development of maritime simulation technologies demonstrates a clear trend toward the integration of cybersecurity as an essential element of maritime safety and professional training. With the increasing digitalization of ship systems, the likelihood of cyberattacks is also increasing. A variety of approaches to achieving the common goal of improving awareness and preparedness of maritime personnel for responding to cyber incidents are demonstrated by platforms such as Cyber-SHIP Lab, Naval Cyber Range, and the CDeX Maritime Cybersecurity Scenario, as well as by industrial solutions such as K-Sim,

NavSim, and SeaSAFER. Each platform offers a different level of technical complexity and applicability within a training context.

Based on these considerations, a comparative analysis of existing simulation platforms is necessary to assess their technical characteristics and educational value in maritime cybersecurity training. This analysis supports the identification of effective approaches and provides the basis for the proposed integrated hybrid simulation model, which combines physical and virtual environments to enhance training effectiveness.

III. RESULTS AND DISCUSSION

A. Comparison of maritime cybersecurity training platforms and simulators

TABLE 1. COMPARATIVE ANALYSIS OF MARITIME CYBERSECURITY TRAINING PLATFORMS AND SIMULATORS

Platform Criteria	Cyber-SHIP Lab	Naval Cyber Range	CDeX Maritime Cybersecurity Scenario	SeaSAFER	NavSim / K-Sim (industry)
Type	Physical hardware laboratory/navigation simulator "ship bridge"	Modular cyber range	Software service in a cyber range based on scenarios	Online training platform	Commercial simulators (hardware and cloud-based)
Realism of the simulation environment	Physical systems, real devices	Real IT/OT infrastructure, PLC	Realistic scenarios	Cases in a virtual environment	Navigation simulators, "ship bridge" and others, cloud-based options and augmented reality
Types of attacks / scope	GPS/AIS spoofing, ECDIS compromise, malware, PLC tests	Wide range of IT/OT: PLC, networks, navigation	Phishing, infected updates, GPS jamming, AIS spoofing	Case study scenarios based on real incidents	Navigation and operational scenarios; possibilities for integrating cybersecurity-related scenarios
Pedagogical approach	Practical exercises, research in a controlled environment	Practical exercises, research in a controlled environment	Role-playing training, operational team exercises	Case-based learning	Combined learning platforms - courses, practical exercises, access to a cloud environment
Target audience	Researchers, students, maritime specialists	Military and civilian personnel, cyber specialists	Maritime crews, ship operators, researchers	Maritime personnel, trainees	Universities, maritime academies, shipping companies, maritime crews, maritime personnel, researchers
Positive aspects	Realistic simulation of a "ship bridge", modern equipment	Modular and flexible cyber range suitable for testing multiple attacks	Realistic scenarios with a variety of attacks, suitable for practical training	Low cost, easy access, certification opportunity	Large-scale solutions, global distribution, support for virtual and learning environments

The following criteria are selected for the comparative analysis of the selected platforms:

- Type - allows technology to be classified according to the degree of physical implementation and infrastructure resources, which is important for assessing its applicability in an educational environment.
- Realism of the simulation environment - in cybersecurity training, the realism of the simulation environment helps students acquire skills that are as close as possible to the real working environment.
- Types of attacks/scope - show how up to date the system is, whether it covers current threats, and what competencies it can develop in learners.
- Pedagogical approach - to be applied in educational programs, the system must include specific learning formats (scenarios, role-playing games, practical exercises) that develop both technical skills and place learners in realistic decision-making situations.
- Target audience - determines who the platform is intended for - students, crews, engineers, officers, etc.
- Positive aspects - highlight the main strengths that make a system effective for training.

The selected criteria combine technical, pedagogical, and applied aspects, which allows for an assessment of the role of simulation technologies in maritime cybersecurity training.

Based on the selected criteria, a comparative analysis of the platforms is presented in Table 1. It shows that maritime cybersecurity training is developing in the direction of combining ship bridge simulators with simulated attacks in a virtual environment. Platforms such as Cyber-SHIP Lab and Naval Cyber Range offer a high level of simulation fidelity through real physical or hybrid infrastructure (IT/OT systems, PLC, navigation equipment), making them suitable for training specialists and conducting experimental research. At the same time, CDeX and SeaSAFER demonstrate a flexible pedagogical model focused on scenario- and role-based training, accessible online and with a lower cost for building the infrastructure itself.

Industrial simulators such as K-Sim offer a high degree of realism in the maritime operating environment, combining traditional bridge training with elements of cybersecurity. This makes them a valuable tool for maritime academies and shipping companies seeking compatibility between classic navigation skills and cyber defense on board.

The analysis shows that training effectiveness increases when simulation environments combine a high degree of realism, scenario-based training, and the ability to reflect real incidents. In terms of target groups, the platforms cover a wide spectrum - from cadets and crews to researchers and military specialists - highlighting the versatility and applicability of the simulation approach in maritime cybersecurity. It can be concluded that a combined model integrating physical and virtual simulations would be highly effective for training purposes, as it supports both technical competence and the development of analytical thinking, which are essential for responding to cyber incidents in the maritime industry.

B. Design of an integrated simulator for maritime cybersecurity training

The proposed integrated simulation model (Fig. 1) includes the main components and interrelationships in the maritime cybersecurity training system and enables work in a hybrid environment. It includes physical infrastructure, virtual environment, communication modules and modules for evaluation and feedback. The aim of the diagram is to present the integration of physical and virtual components, to show the flow of information and interactions between the system and trainees, and to demonstrate how simulation develops technical and operational skills for recognizing, responding to, and controlling cyber threats in a safe and controlled environment.

The physical environment contains bridge, engine room, IT/OT systems, navigation and communication systems. Based on this, students can develop competencies in technical skills, critical thinking, physical feedback, and muscle memory. The results of the student's actions are assessed and analyzed by a module for the assessment and analysis of physical competencies.

The virtual environment contains cyber range, scenarios, simulated attacks, VR/AR. Based on this, students can acquire the skills to detect and analyze threats, classify incidents, and work with cybersecurity software. The results of the students' actions are assessed and analyzed by a module designed to evaluate and analyze the skills acquired in a virtual environment.

Trainees from different environments can exchange information in a virtual environment. They can compare data from the compromised system with that from the physical system to identify the source of a malfunction on the ship, which may be mechanical or due to external interference.

Cross-validation in physical and virtual learning environments is a process of mutual verification and confirmation of the knowledge and skills gained in both environments. The knowledge gained through virtual simulations is applied and tested in the physical environment, and the results from practical tests are then compared with the virtual models. This two-way

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.114>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

assessment determines how effective the skills are, identifies discrepancies, and allows for adjustments, leading to a more secure, accurate, and lasting retention of knowledge.

The assessment of competencies in a hybrid environment includes team communication between participants, real-time risk assessment, prioritization of crew actions, and working under critical conditions. Competency assessment can be performed automatically or

by the instructor. The calculated grade for automated competency assessment includes:

- Trainees response time upon detecting a vulnerability.
- Accuracy of the sequence of actions taken to prevent the incident.
- Condition of the ship's physical parameters during and after the cyberattack.

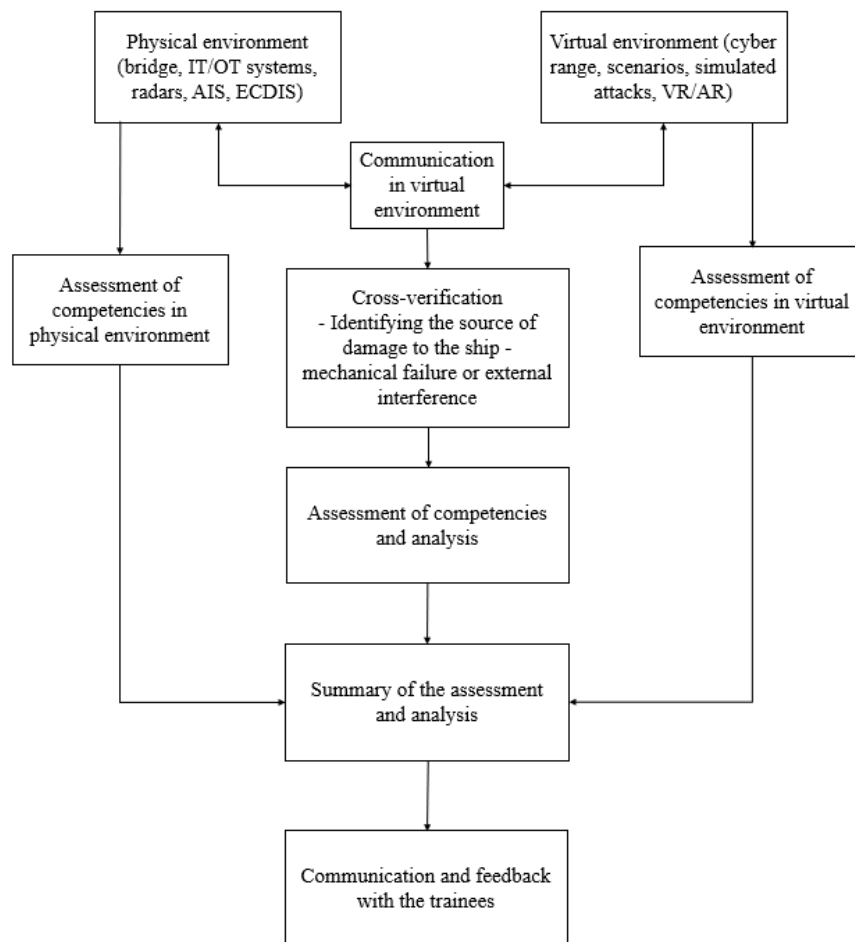


Fig. 1. Integrated model of a simulator for maritime cybersecurity training

The instructor observes the trainee's actions and conducts a post-session review of:

- Communication during the attack.
- The effectiveness of decision-making during the process of preventing the attack.
- Analysis of the mistakes made by the trainees.

The results of the assessment of competencies in the physical environment, the virtual environment, and communication in the virtual environment are summarized and analyzed. This allows for tracking of trainees progress,

identification of their strengths and areas for improvement, and the implementation of appropriate measures to enhance the effectiveness of the training process. Timely and constructive feedback is also provided to students, which supports their development and improvement.

The proposed integrated hybrid simulation model provides a comprehensive and effective framework for the development, assessment, and continuous improvement of maritime cybersecurity competencies within a realistic and controlled training environment.

IV. CONCLUSIONS

As part of organizational risk management processes, staff training is essential. The goal is to ensure that all employees acquire the knowledge and skills needed to recognize and manage risks arising from the use of various technologies. Effective training and awareness are key elements in building comprehensive cyber resilience in the maritime industry.

Simulation technologies have become an important tool for maritime cybersecurity training, providing a safe and controlled environment for developing technical skills, analytical thinking, and coordinated responses to cyber incidents. Comparative analysis shows that platforms combining physical ship systems with virtual cyberattack scenarios are highly effective, as they offer both realism and opportunities to practice responses in conditions close to real operations. Platforms such as Cyber-SHIP Lab and Naval Cyber Range demonstrate strong technical reliability and support experimental research, while solutions like CDeX and SeaSAFER offer flexibility, lower cost, and accessibility. Industrial simulators such as K-Sim integrate traditional maritime training with cybersecurity components, enabling large-scale training aligned with international standards. Overall, a hybrid approach that integrates physical and virtual simulation appears to be the most effective for preparing maritime personnel to address modern cyber threats.

The proposed integrated simulation model demonstrates that combining physical ship infrastructure with a virtual cyber environment can significantly enhance training effectiveness. By linking real ship systems with cyber range scenarios, simulated attacks, and VR/AR technologies, the model supports the development of both technical and operational competencies. It facilitates individual skill acquisition, critical thinking, decision-making, and teamwork under realistic conditions. A key contribution of the model is cross-validation between physical and virtual environments, where knowledge gained in one setting is tested and reinforced in the other. This approach improves assessment accuracy, identifies competency gaps, and strengthens long-term knowledge retention. The integrated evaluation framework combines automated performance metrics with instructor-led assessment, ensuring a comprehensive evaluation of trainee performance.

The results of the comparative analysis and the proposed framework confirm that hybrid simulation-based training systems offer high realism, flexibility, and analytical capability. They support effective progress tracking, targeted feedback, and continuous competency development. Therefore, an integrated hybrid simulation approach represents a scalable and resilient solution for preparing maritime personnel to respond effectively to evolving cyber threats in complex operational environments.

ACKNOWLEDGMENTS

This report was financed by the Ministry of Education and Science under the National Science Program "Security

and Defense", carried out in implementation of the National Strategy for the Development of Scientific Research 2017-2030 and adopted by Decision of the Council of Ministers No. 731 of October 21, 2021. The material reflects only the author's opinion and the Ministry of Education and Science is not responsible for the content.

REFERENCES

- [1] Y. Kong, "The Role of Experiential Learning on Students' Motivation and Classroom Engagement," *Front. Psychol.*, vol. 12, p. 771272, Oct. 2021, <https://doi.org/10.3389/FPSYG.2021.771272>.
- [2] M. H. Dewan, R. Godina, M. R. K. Chowdhury, C. W. M. Noor, W. M. N. Wan Nik, and M. Man, "Immersive and Non-Immersive Simulators for the Education and Training in Maritime Domain—A Review," *Journal of Marine Science and Engineering* 2023, Vol. 11, Page 147, vol. 11, no. 1, p. 147, Jan. 2023, <https://doi.org/10.3390/JMSE11010147>.
- [3] STCW online, "STCW Safety Officer on Board Online Course," https://stcw.online/course/safety-officer-on-board/?utm_source=google&utm_medium=cpc&utm_campaign=Search_Low_Priority_Courses_High_Conversion&utm_id=21488347567&utm_term=186364137043_ship%20safety%20training&utm_content=778296802923&gad_source=1&gad_campaignid=21488347567&gbraid=0AAAAADhSnhiAlJoXsQURbFdN8yuuD782O&gclid=CjwKCAjwqazPBhALEiwAOuXqdJJKQ6JcPdMVOWHvJ1LFIT_mRKEyXDPIOn_hWPSllw62B4YQq3_sxxoC10wQAvD_BwE.
- [4] [Nikola Vaptsarov Naval Academy, "Simulation engineering," www.naval-acad.bg. Accessed: Apr. 24, 2026. [Online]. Available: <https://www.naval-acad.bg/application/majors/master/simulation-engineering>
- [5] P. Ruponen, E. Altintas, J. Matusiak, and T. Mikkola, "A practical approach for simplified operational guidance to avoid parametric roll resonance," *Ocean Engineering*, vol. 330, Jun. 2025, <https://doi.org/10.1016/j.oceaneng.2025.121215>.
- [6] [Y. Eustache, C. Seguin, A. Pecout, A. Foucher, J. Laurent, and D. Heller, "Marine Object Detection Using LiDAR on an Unmanned Surface Vehicle," *IEEE Access*, vol. 13, pp. 121658–121669, 2025, <https://doi.org/10.1109/ACCESS.2025.3587315>.
- [7] A. M. A. Reverón, C. E. M. Luis, and J. M. Gutiérrez, "NavAR, an App for Training in Cartography and Maritime Navigation Through Augmented Reality," in *Lecture Notes in Mechanical Engineering*, San Cristóbal de La Laguna: Springer Science and Business Media Deutschland GmbH, 2024, pp. 319–329. https://doi.org/10.1007/978-3-031-51623-8_31.
- [8] Y. Bohdan, I. Bohomolova, A. Satulov, S. Voloshynov, and V. Savchuk, "COMPARATIVE ANALYSIS FOR STATE-OF-THE-ART SIMULATION TRAINING SYSTEMS THOSE INFLUENCE ONTO THE FUTURE ENGINEERS' KNOWLEDGE AND SKILLS," in *21st Annual General Assembly, IAMU AGA 2021 - Proceedings of the International Association of Maritime Universities, IAMU Conference, Kherson*, 2021. Accessed: Nov. 11, 2025. [Online]. Available: <https://www.scopus.com/pages/publications/85124620290?origin=resultlist>
- [9] J. Orović, M. Valčić, V. Knežević, and Z. Pavin, "Comparison of the on Board Measured and Simulated Exhaust Gas Emissions on the Ro-Pax Vessels," *Atmosphere (Basel)*, vol. 13, no. 5, May 2022, <https://doi.org/10.3390/atmos13050794>.
- [10] M. Nikolova, E. Andreev, and Y. Kolarov, "Creation of Scenarios with VSTEP Simulator and Evaluation of Simulators Use in Maritime Education and Training," *Scientific Bulletin of Naval Academy*, vol. XXVI, pp. 64–72, 2023, <https://doi.org/10.21279/1454-864X-23-I2-007>.
- [11] University of Plymouth, "Maritime cyber threat mitigation training - University of Plymouth," Maritime cyber threat

- mitigation training. Accessed: Oct. 03, 2025. [Online]. Available: <https://web.archive.org/web/20250615142908/https://www.plymouth.ac.uk/research/cyber-ship-lab/maritime-cyber-threat-mitigation-training>
- [12] Naval Systems Cyber Defense Chair, “Cyberrange | Chaire de Cyberdéfense des Systèmes Navals,” cyberrange. Accessed: Oct. 03, 2025. [Online]. Available: <https://web.archive.org/web/20250719120754/https://chaire-cyber-navale.fr/en/cyberrange/>
- [13] Naval Systems Cyber Defense Chair, “Advanced simulation platform for cyber security of maritime systems.” Accessed: Nov. 07, 2025. [Online]. Available: <https://web.archive.org/web/20251107135426/https://chaire-cyber-navale.fr/en/cyberrange/>
- [14] CDEX, “Defending the Seas — CDeX’s Maritime Cybersecurity Scenario,” Defending the Seas — CDeX’s Maritime Cybersecurity Scenario. Accessed: Oct. 03, 2025. [Online]. Available: <https://cdex.cloud/blog/technology-updates/defending-the-seas-cdexs-maritime-cybersecurity-scenario/>
- [15] CDEX, “Discover the Power of CDeX Training Catalogue.” Accessed: Nov. 07, 2025. [Online]. Available: <https://cdex.cloud/blog/technology-updates/discover-the-power-of-cdex-training-catalogue/>
- [16] Kongsberg Maritime, “Simulation - Kongsberg Maritime,” Simulation. Accessed: Oct. 06, 2025. [Online]. Available: <https://web.archive.org/web/20250518200707/https://www.kongsberg.com/maritime/products/simulation/>
- [17] Wärtsilä, “Wärtsilä Navigational simulators,” www.wartsila.com. Accessed: Oct. 03, 2025. [Online]. Available: <https://web.archive.org/web/20250905015437/https://www.wartsila.com/marine/products/simulation-and-training/navigational-simulators>
- [18] SeaSAFER, “SeaSAFER Background,” SeaSAFER.com. Accessed: Oct. 03, 2025. [Online]. Available: <https://web.archive.org/web/20251003123235/https://seasafer.com/bg/>

Design and Scenario Development of a Maritime Cybersecurity Training Simulation Platform

Ekaterina Dyankova

Department of Information
Technologies

Nikola Vaptsarov Naval Academy
Varna, Bulgaria

edyankova@naval-acad.bg

Dilyana Dimitrova

Department of Information
Technologies

Nikola Vaptsarov Naval Academy
Varna, Bulgaria

di.dimitrova@naval-acad.bg

Evgeni Andreev

Department of Information
Technologies

Nikola Vaptsarov Naval Academy
Varna, Bulgaria

e.andreev@naval-acad.bg

Abstract— This paper presents the design and scenario development of a simulation platform for maritime cybersecurity training. In response to the increasing digitalization of shipboard systems and the growing exposure to cyber threats, the platform provides a web-based environment that simulates a ship bridge and enables hands-on training in cyber incident response. The system supports real-time interaction with key on-board systems, allowing users to observe and respond to unusual behavior under simulated attack conditions. The platform includes three cyber-physical scenarios: GPS spoofing, AIS data injection, and engine control malware. The presented solution is designed to respond to specific training needs - the detection of cyber-physical attacks in conditions that closely simulate real-life scenarios. It is suitable for integration into academic and professional maritime training, enhancing traditional bridge simulators by addressing specific cybersecurity challenges in a controlled and accessible environment.

Keywords— maritime cybersecurity, simulation-based training, ship bridge simulation.

I. INTRODUCTION

The rapid adoption of digital technologies in the maritime sector is transforming the way modern vessels are navigated, operated, and maintained. Systems like Electronic Chart Display and Information System (ECDIS), Automatic Identification System (AIS) and Integrated Bridge Systems (IBS) are turning ship operations into complex cyber-physical processes in which the human factor interacts with automated digital solutions [1]. This digitalization is leading to a new era of maritime safety, the need for cyber resilience and the ability to respond to digital incidents [2].

At the same time, maritime education is going through a significant change. The integration of simulation technologies as a primary training method provides an opportunity to gain practical experience in performing complex operations in a controlled environment, without risk to personnel or equipment [1], [3]. In parallel, cybersecurity training has become essential for protecting

maritime operations, safeguarding sensitive information, ensuring regulatory compliance, and reducing the financial and operational risks associated with cyber threats. As a result, cybersecurity competence is now a key component of the resilience and security of the global maritime industry [4].

The introduction of maritime cyber simulators represents the next stage in the development of simulation technologies. They combine the physical infrastructure of a ship's bridge with virtual cyber scenarios, allowing trainees to study how systems behave when exposed to threats such as malware, GPS spoofing, and unauthorized access to on-board networks [5]. In this way, simulation environments have become a tool for technical training and a means of developing critical thinking, situational awareness, and coordination skills in crisis situations. As a result, they play a dual role in modern maritime education: on the one side, they support the development of professional competencies related to the safety and efficiency of maritime operations, and on the other, they develop the cognitive and social skills necessary for managing cyber risks in the digitalized maritime environment.

Recent studies have examined the issue of maritime cybersecurity training and the need to develop maritime cybersecurity simulators. Publications in the global Scopus database from the past five years were analysed. The search utilized the keywords "maritime", "simulators", and "cybersecurity." Six publications were selected that met the specified criteria and addressed the topic of the problem under consideration.

In paper [6], the authors investigate the vulnerabilities of the ship's main engine lubrication system using a MATLAB Simulink model, simulate various scenarios, and evaluate the system's behavior. The study demonstrates how cyberattacks on sensors and controllers can lead to critical temperature deviations, potentially causing engine damage. This work highlights the need to integrate cyber scenarios into physical simulators for crew

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.116>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

training, with the aim of developing critical thinking and incident response capabilities. In [7], ShipNetSim is developed - an open-source simulator that combines aspects of environmental science and cybersecurity, expanding the scope of maritime cybersecurity training, particularly in the assessment of GPS spoofing and route optimization. In [8], the authors present ICoSSiuM, a simulator focused on maritime communications, primarily the AIS. The simulations demonstrate how attacks on communication systems can disrupt maritime operations, adding another aspect to maritime cybersecurity. Through simulated cyberattack scenarios (tabletop exercises), exercises on navigation simulators, and questionnaires, the authors in [9] find that future navigators of unmanned vessels will require training that includes new skills for interacting with digital systems in various activities, such as remote monitoring and others, in order to overcome various challenges, including the management of cyber incidents. In their publication [10], the authors examine autonomous vessels and present a modular warship simulator with artificial intelligence-based monitoring for navigation and network operations. The simulation includes GPS spoofing and attacks on industrial control systems. These technologies aim to train personnel to detect anomalies and protect the ship, demonstrating the potential of artificial intelligence in cyber simulation training. The authors in [11] developed MaCySTe, a project providing a test environment that simulates network infrastructure and the main components of ship cyber-physical systems and integrates with ship simulators. The platform provides realistic training and testing of countermeasures, thereby enhancing the cybersecurity culture among the crew.

Based on the analysis of the literature, it can be concluded that simulation technologies are established as a key tool in the training of maritime personnel, particularly in the context of growing cyber threats to ship systems and communications. They enable the practical learning of a variety of skills in a safe environment, such as responding to cyberattacks on physical and communication systems on board. Combining various aspects of maritime cybersecurity can prepare personnel for real-world operations and incidents.

The main aim of the paper is to present the design and scenario development of a simulation platform for maritime cybersecurity training. The presented solution is designed to respond to specific training needs - the detection of cyber-physical attacks in conditions that closely simulate real-life scenarios.

II. MATERIALS AND METHODS

A. The evolution of maritime simulators over the years

The development of simulation technologies related to maritime education is illustrated in Fig. 1.

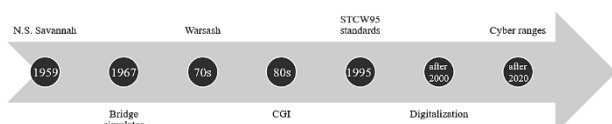


Fig. 1. The development of simulation technologies in maritime education.

The concept of simulation in maritime training goes back to the mid-20th century. A pioneering step can be linked to the world's first nuclear-powered merchant ship, the N.S. Savannah (1959). It is noted that a computer-based training system was used for the crew [12]. However, there is not enough data to confirm that this was a complete computer simulator.

Two key developments emerged in the 1960s. In 1967, the first modern ship bridge simulator was built in Gothenburg, Sweden, to study crew behavior, ship architecture, and port design [13]. By the end of the decade, several countries (Sweden, the Netherlands, the United States, and Japan) had developed their own ship maneuvering simulators, initially intended primarily for scientific research. The first practical training simulators appeared in the early 1970s. The first "bridge" simulator in the United Kingdom was developed at the Warsash School of Maritime Studies and used projected dots of red, green, and white lights to represent approaching ships and buoys [12]. It quickly established itself as a leading innovation in maritime training for its time, proving its effectiveness. Over time, these early analog systems evolved into digital simulators with increasingly realistic graphics and multidisciplinary applications.

During the 1970s and 1980s, simulation technology evolved rapidly. Simulators, such as the one in Warsash, were replaced by computer-controlled systems with black-and-white and, later, color graphics. In 1982, the first simulator with computer-generated imagery (CGI) for day and night graphics was developed in the United Kingdom. At the same time, a simulator based on aviation technology (Computer Aided Operations Research Facility - CAORF) was introduced at the Naval Academy in New York, USA, used for scientific research and for training cadets [12].

At the end of the 20th and beginning of the 21st centuries, advances in computer and graphics processor technology made it possible to integrate complex navigation systems (ECDIS, GPS, radar, and others) into simulators. According to [14], following the adoption of the new STCW95 requirements (1995, effective 1997) and due to technologies from the video game industry, maritime training now utilizes multi-platform solutions: stationary and fully functional navigation simulators, desktop and cloud-based simulators, as well as virtual and augmented reality applications [13], [14]. According to leading manufacturers such as Wärtsilä (NavSim), their simulation systems support training in both traditional classrooms and VR/AR environments, as well as network architectures for distributed learning, all unified under a single software package [15]. High realism is achieved through authentic ship models, classrooms featuring detailed replicas of bridges and engine rooms, dynamic maritime environments, and, when necessary, the movement of simulated ships (dynamic positioning, etc.).

Tracking the evolution of simulation technologies in maritime training reveals a consistent progression from

analog systems with limited visual capabilities to realistic digital environments that integrate navigation and communication components, as well as the inclusion of cyberattack simulations. From the first experimental simulators in the 1960s to modern VR/AR and cloud-based platforms, the trend has been toward increasing the realism, safety, and effectiveness of training. These technologies optimize the training process for maritime professionals, create conditions for adapting to new challenges, and lead to the development of new solutions capable of simulating real-time attacks to improve trainees' decision-making skills.

B. Design of a maritime cybersecurity training simulation platform

The developed web-based training environment simulates the bridge of a cargo ship. The idea is to offer an accessible and easily deployable tool that meets the IMO's requirements for cyber risk management [16] and the NIST cybersecurity framework (CSF) [17]. It operates entirely on the client side, enabling accessibility through standard web browser without requiring dedicated infrastructure. The goal is the trainees to be able to recognize the symptoms of three types of cyber-physical attacks in real time, apply the correct mitigation procedures, see the immediate effect of their actions, and understand what happens when they make the wrong decision.

The platform is developed for cadets, students and officers at the Nikola Vaptsarov Naval Academy in Varna, Bulgaria, but it is also applicable in other maritime higher education institutions or corporate crew training programs.

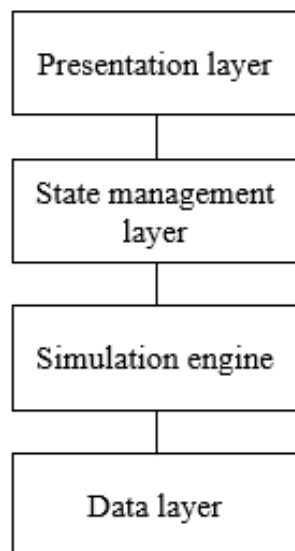


Fig. 2. System architecture.

The system architecture is presented in Fig. 2. It is organized into four logical layers:

- presentation layer - it consists of interactive user interface components that visually represent ship systems and operational conditions;

- state management layer - maintains the global simulation state, which includes system integrity, active threats, user progress, and event logs;
- simulation engine - it controls the execution of cyberattack scenarios, handling user interactions, validating responses, and updating system behavior;
- data layer - provides configurable definitions of attack scenarios and enables flexibility and extensibility without modifying core application logic.

Following the description of the four architectural layers, the technological foundation of each layer is presented to provide a complete picture of the implementation. The platform is developed as a single-page application using React 19 with TypeScript, with Vite serving as the build toolchain. TypeScript is selected to ensure static type safety across the simulation state model, where typed interfaces define system statuses, challenge-step structures, and attack scenario configurations.

The presentation layer is styled with Tailwind CSS as a utility-first framework and includes Framer Motion for animated transitions, including alert pulsations, radar scan-line effects, and modal interactions, while Lucide React supplies consistent SVG iconography across the interface. The state management layer is implemented through React's built-in hooks (useState, useEffect), maintaining a single SimulationState object that encapsulates active attack references, ship system parameters, event logs, score, elapsed time, and integrity values. The simulation engine operates through a one-second interval timer that decrements vessel integrity during active attacks, applies pseudorandom fluctuations to compromised sensor readings, and evaluates termination conditions. The data layer is implemented as a declarative TypeScript module defining scenario parameters, challenge steps, valid responses, and penalty structures.

At the core of the platform is a centralized simulation controller that orchestrates the execution flow. Each training scenario is modelled as a sequence of structured steps representing different stages of a cyberattack. Users interact with the system through decision panels, where their actions are evaluated in real time. Correct responses advance the simulation and improve performance metrics, while incorrect actions result in penalties such as reduced system integrity or degraded system functionality. The application runs entirely client-side without server-side components or external API dependencies, requiring only Node.js (version 18 or higher) as a development-time dependency. This deployment model ensures accessibility in maritime training environments with limited or restricted network connectivity.

The platform also includes a system visualization module that mimics real maritime interfaces and includes radar displays and subsystem panels. These components dynamically reflect the effects of cyberattacks, enhancing situational awareness. An event logging mechanism

records all actions and system changes, providing immediate feedback during execution and supporting post-simulation analysis.

The system workflow (Fig. 3) begins with scenario initialization, followed by stepwise user interaction, real-time evaluation, and continuous feedback. The simulation terminates either upon successful completion of all steps or when system integrity falls below a defined threshold. The current design emphasizes simplicity and accessibility. The interface of the simulation platform is presented in Fig. 4.

A key design feature is the use of a configurable data model for defining attack scenarios. Each scenario specifies targeted systems, ordered challenge steps, and possible incorrect actions with associated consequences. This approach allows domain experts to extend the platform with new threat scenarios without altering the underlying implementation, improving maintainability and scalability.

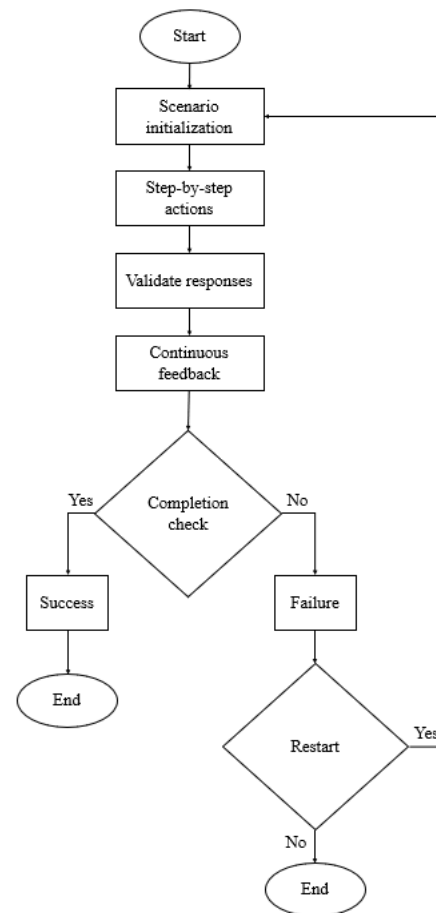


Fig. 3. System workflow.

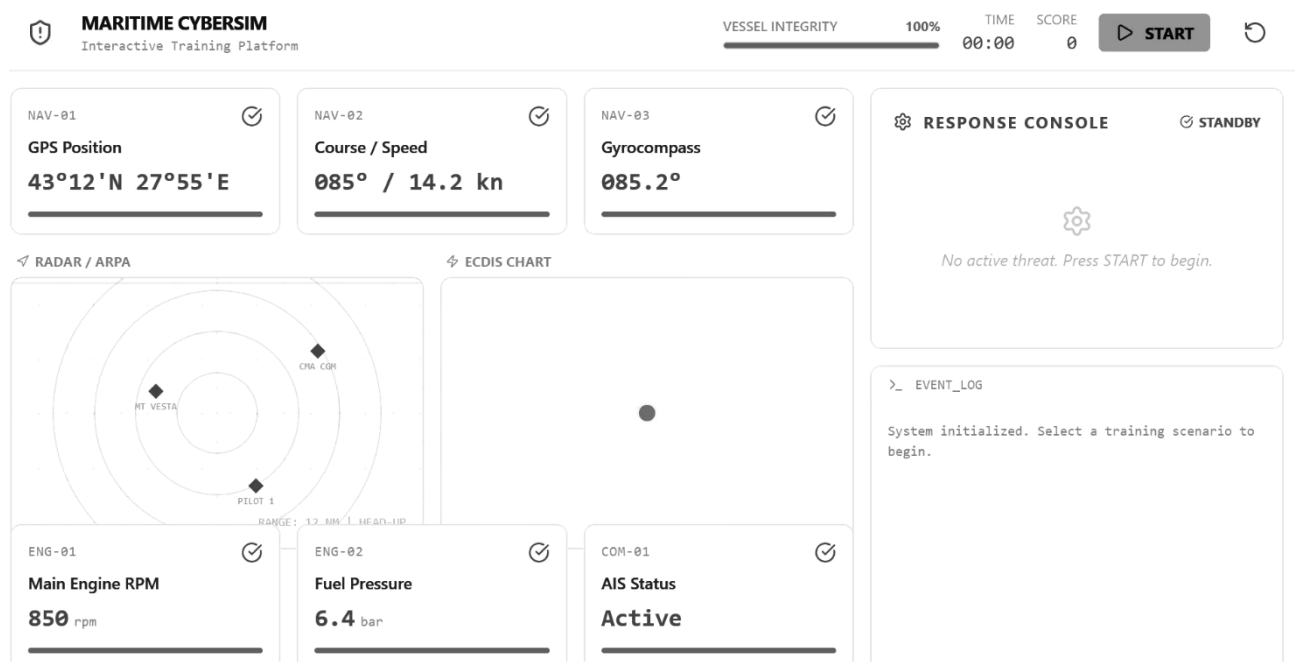


Fig. 4. The interface of the simulation platform.

III. RESULTS AND DISCUSSION

Select Training Scenario

Each scenario requires hands-on problem solving — not just button clicks.

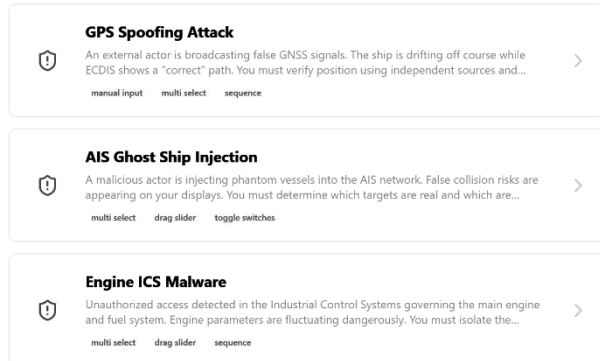


Fig. 5. Scenario options.

The proposed solution includes three cyber-physical attack scenarios presented in Fig. 5, each reflecting a distinct category of maritime cybersecurity threat and grounded in both real-world incidents and documented vulnerabilities in the literature. They are designed to simulate realistic on-board conditions, requiring trainees to detect anomalies, assess system reliability, and execute appropriate mitigation procedures. The scenarios provide structured learning progression from navigation data manipulation to direct compromise of critical control systems.

A. GPS spoofing attack scenario

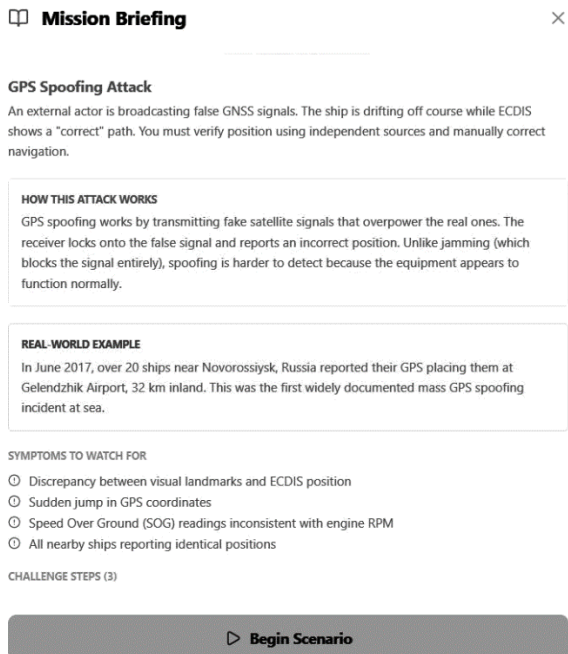


Fig. 6. Scenario 1 overview.

The first scenario models a GPS (Global Positioning System) spoofing attack, in which spoofed satellite signals are transmitted to override legitimate positioning data. As a result, the vessel appears to maintain a valid position on the Electronic Chart Display and Information System (ECDIS), while it deviates from its intended course. This type of attack has been documented in operational environments, most notably in the Black Sea incident in June 2017, where more than 20 vessels near Novorossiysk reported false GPS positions directing them inland toward Gelendzhik airport [18]. More recent observations in the period 2023-2024 further confirm that GNSS (Global Navigation Satellite System) spoofing has evolved into an operational threat [19]. Fig. 6 presents an overview of a GPS spoofing attack scenario. The panel includes a real-world example, lists warning signs, and outlines steps to verify and correct navigation before starting the scenario.

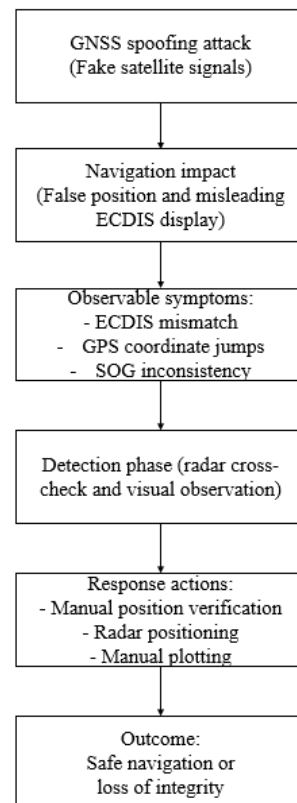


Fig. 7. GPS spoofing attack workflow.

Within the simulation, a GNSS spoofing attack causes false position data, coordinate jumps, and inconsistencies in course over ground (COG) and speed over ground (SOG). As shown in Fig. 7, trainees must detect discrepancies between GNSS data and independent sources to maintain situational awareness and safe navigation.

B. AIS ghost ship injection scenario

The second scenario presented in Fig.8 simulates an AIS data injection attack, where an adversary introduces altered vessel information into the communication network, resulting in the appearance of non-existent targets (“ghost ships”). This type of manipulation exploits the lack of authentication and encryption in AIS protocols, making them inherently vulnerable to spoofing and data injection attacks.

Mission Briefing

AIS Ghost Ship Injection

A malicious actor is injecting phantom vessels into the AIS network. False collision risks are appearing on your displays. You must determine which targets are real and which are fabricated.

HOW THIS ATTACK WORKS

AIS operates on unencrypted VHF radio. Anyone with cheap equipment can broadcast false AIS messages, creating “ghost ships” that appear on every nearby vessel’s display. These phantom targets can trigger collision alarms and cause dangerous evasive maneuvers.

REAL-WORLD EXAMPLE

Between October 2022 and April 2023, AIS spoofing incidents surged by 400% globally, driven largely by sanctions evasion. Ghost ship patterns have been documented creating “Z” symbols in the Black Sea.

SYMPTOMS TO WATCH FOR

- ⊙ Targets visible on AIS but absent from Radar
- ⊙ Vessels performing physically impossible maneuvers
- ⊙ Multiple targets sharing the same MMSI number
- ⊙ Targets appearing/disappearing suddenly

Begin Scenario

Fig. 8. Scenario 2 overview.

Such incidents are reported in practice. For example, analyses of maritime traffic data indicate a significant rise in AIS spoofing events, with reported cases increasing by up to 400% between late 2022 and early 2023. Other studies further confirm that AIS messages can be easily forged, allowing attackers to create phantom vessels, duplicate identities, or manipulate vessel trajectories [20].

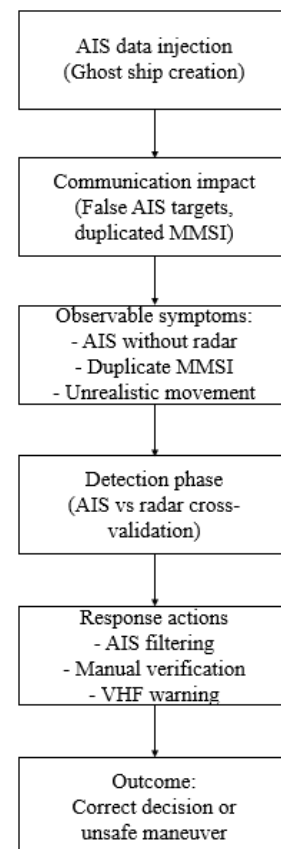


Fig. 9. AIS ghost ship injection workflow.

In the simulation, ghost targets appear on the AIS display without corresponding radar echoes or exhibit anomalies such as duplicated Maritime Mobile Service Identity (MMSI) numbers and unrealistic movements (Fig. 9). Trainees must identify these inconsistencies by correlating AIS data with radar and visual observations. The scenario trains users to apply filtering mechanisms, switch to manual verification modes, and prioritize trusted sensor inputs. It also incorporates communication procedures, such as issuing navigational warnings. The objective is to prevent unsafe decisions, particularly unnecessary evasive maneuvers triggered by falsified information.

C. Engine ICS malware scenario

✎ Mission Briefing

Engine ICS Malware

Unauthorized access detected in the Industrial Control Systems governing the main engine and fuel system. Engine parameters are fluctuating dangerously. You must isolate the infected segments and restore manual control.

HOW THIS ATTACK WORKS

Ship engine rooms run on Industrial Control Systems (ICS) connected to the bridge via internal networks. If malware reaches these systems, it can manipulate fuel injection, RPM limiters, and temperature sensors. Unlike IT attacks, ICS compromise has immediate physical consequences.

REAL-WORLD EXAMPLE

The 2017 NotPetya attack devastated Maersk's operations for two weeks, affecting 76 port terminals and costing approximately \$300 million. The malware spread through a Ukrainian accounting software update.

SYMPTOMS TO WATCH FOR

- ⊖ Throttle commands not responding
- ⊖ Fuel pressure fluctuating without physical cause
- ⊖ Engine temperature warnings with no actual overheating

▶ Begin Scenario

Fig. 10. Scenario 3 overview.

The third scenario addresses a malware attack targeting industrial control systems (ICS) within the vessel's engine and propulsion subsystem (Fig. 10). This case represents a direct compromise of operational control, posing an immediate risk to vessel safety.

The relevance of such attacks is supported by increasing concerns in the maritime domain regarding vulnerabilities in operational technology (OT) systems. International guidelines, including those issued by the International Maritime Organization (IMO), highlight the growing risk of cyber incidents affecting shipboard control systems [16].

In the simulation, the attack results in unstable engine behaviour - fluctuating revolutions per minute (RPM), irregular fuel pressure, and unresponsive control inputs (Fig. 11). Trainees must identify compromised network segments based on abnormal traffic patterns and they need to isolate affected systems so they can prevent further propagation. The response process includes transitioning to manual control, verifying system states through local instrumentation, and executing a controlled recovery sequence. The scenario emphasizes important cybersecurity principles such as network segmentation, incident containment, and staged system restoration and illustrates the risks associated with improper actions during an active attack.

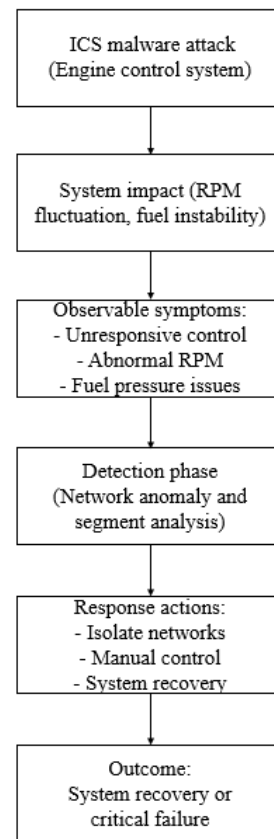


Fig. 11. Engine ICS malware scenario workflow.

The platform provides an accessible and flexible training solution compared to existing large-scale simulators. Its main advantage is the web-based architecture and ease of deployment. Despite its advantages, the current implementation has certain limitations which include the absence of real hardware integration and a limited set of training scenarios. The platform does not claim to replace full-scale bridge simulators, but it fills a niche that they don't cover - training in responding to cyber incidents in which navigation sensors malfunction, engine controllers fail to respond, and simulated ships threaten to collide. Possible directions for future development include adding new scenarios, introducing difficulty levels, a multiplayer mode, and integration with real NMEA data from navigation simulators.

IV. CONCLUSIONS

The paper presents the design and scenario development of a web-based maritime cybersecurity training simulation platform aimed at improving the preparedness of maritime personnel for cyber-physical incidents. The proposed solution provides an accessible and interactive environment that enables users to observe, analyze, and respond to cybersecurity threats affecting critical shipboard systems.

The platform integrates a modular architecture and a configurable scenario model, allowing the simulation of realistic cyberattack situations without the need for

specialized hardware. Three scenarios (GPS spoofing, AIS data injection, and engine ICS malware) were implemented to reflect key categories of maritime cyber threats, ranging from navigation manipulation to direct control system compromise. They support the development of essential skills such as anomaly detection, decision-making under uncertainty, and application of mitigation procedures.

The results demonstrate that the platform can serve as a valuable addition to traditional maritime simulators by introducing training focused on cybersecurity in a flexible and scalable format. Its web-based nature enables easy deployment in both academic and professional training environments, making it particularly suitable for institutions with limited access to full-scale simulators.

Future work will focus on expanding the scenario library, including multi-user and collaborative training capabilities, and integrating performance tracking and adaptive learning mechanisms. The proposed platform contributes to bridging the gap between theoretical cybersecurity knowledge and practical maritime training, supporting the development of cyber-resilient maritime operations in an increasingly digitalized industry.

ACKNOWLEDGMENTS

This report was financed by the Ministry of Education and Science under the National Science Program "Security and Defense", carried out in implementation of the National Strategy for the Development of Scientific Research 2017-2030 and adopted by Decision of the Council of Ministers No. 731 of October 21, 2021. The material reflects only the author's opinion, and the Ministry of Education and Science is not responsible for the content.

REFERENCES

- [1] E. Demirel, "Maritime Education and Training in the Digital Era," *Universal Journal of Educational Research*, vol. 8, no. 9, pp. 4129–4142, Sep. 2020, <https://doi.org/10.13189/UJER.2020.080939>.
- [2] F. Martínez, L. E. Sánchez, A. Santos-Olmo, D. G. Rosado, and E. Fernández-Medina, "Maritime cybersecurity: protecting digital seas," *International Journal of Information Security*, vol. 23, no. 2, pp. 1429–1457, Jan. 2024, <https://doi.org/10.1007/S10207-023-00800-0>.
- [3] B. Nikolov, "Approach to developing a maritime cybersecurity virtual training environment," in *Proc. Int. Sci. Practical Conf. Environment. Technology. Resources*, Rezekne, Latvia, Jun. 2024, pp. 220–225, <https://doi.org/10.17770/ETR2024VOL2.8039>.
- [4] B. Nikolov and D. Nikolov, "A Scenario-based approach to cybersecurity training for Seafarers," in *Proceedings of the International Association of Maritime Universities Conference, Buzzards Bay: International Association of Maritime Universities*, 2024, pp. 385–390. Accessed: May 21, 2026. [Online]. Available: <https://aga24.maritime.edu/wp-content/uploads/IAMUC-2024-proceedings-final-corrected.pdf>
- [5] G. Potamos, E. Stavrou, and S. Stavrou, "Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis," *Sensors*, vol. 24, no. 11, May 2024, <https://doi.org/10.3390/S24113458>.
- [6] Y. Gülmez, O. Konur, M. Erbas, and S. Bauk, "Identifying cyber attack vulnerabilities in the main lubricating oil system of marine propulsion units," *International Journal of Critical Infrastructure Protection*, vol. 51, Dec. 2025, <https://doi.org/10.1016/j.ijcip.2025.100810>.
- [7] A. Aredah and H. A. Rakha, "ShipNetSim: An Open-Source Simulator for Real-Time Energy Consumption and Emission Analysis in Large-Scale Maritime Networks," *J. Mar. Sci. Eng.*, vol. 13, no. 3, Mar. 2025, <https://doi.org/10.3390/jmse13030518>.
- [8] L. Bayou, A. Awarkeh, M. E. H. Haouari, R. Yaich, and M. A. Faillon, "ICoSSiuM: An integrated communication security simulator for maritime operations," *Lecture Notes in Computer Science*, vol. 15532, pp. 58–73, 2025, https://doi.org/10.1007/978-3-031-87499-4_5.
- [9] J. D. Palbar Misas, R. Hopcraft, K. Tam, and K. Jones, "Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness," *Journal of Marine Engineering and Technology*, vol. 23, no. 3, pp. 224–235, May 2024, <https://doi.org/10.1080/20464177.2024.2330176>.
- [10] L. Rivas et al., "Assuring Safe Navigation and Network Operations of Autonomous Ships," *IEEE 14th Annu. Comput. Commun. Workshop Conf. (CCWC)*, 2024, pp. 138–143, 2024, <https://doi.org/10.1109/CCWC60891.2024.10427933>.
- [11] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo, "MaCySTe: A virtual testbed for maritime cybersecurity," *SoftwareX*, vol. 23, p. 101426, Jul. 2023, <https://doi.org/10.1016/j.softx.2023.101426>.
- [12] Nautilus International Maritime Union, "Simulators: 45 years of development and debate." Accessed: Apr. 21, 2026. [Online]. Available: <https://web.archive.org/web/20251216032850/https://www.nautilusint.org/en/news-insight/telegraph/simulators-45-years-of-development-and-debate/>
- [13] M. H. Dewan, R. Godina, M. R. K. Chowdhury, C. W. M. Noor, W. M. N. Wan Nik, and M. Man, "Immersive and non-immersive simulators for the education and training in maritime domain-A review," *J. Mar. Sci. Eng.*, vol. 11, no. 1, p. 147, 2023, <https://doi.org/10.3390/jmse11010147>.
- [14] B. Lintott, "The History and Heritage of the Age of Simulation," *Human Factors and Simulation*, vol. 83, 2023, <https://doi.org/10.54941/ahfe1003581>.
- [15] Wärtsilä, "Wärtsilä Navigational simulators." Accessed: Apr. 21, 2026. [Online]. Available: <https://web.archive.org/web/20250905015437/https://www.wartsila.com/marine/products/simulation-and-training/navigational-simulators>
- [16] IMO, "Maritime cyber risk." Accessed: Apr. 22, 2026. [Online]. Available: <https://web.archive.org/web/20260419071845/https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx>
- [17] NIST, "The NIST Cybersecurity Framework." Accessed: Apr. 22, 2026. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [18] M. Jones, "Spoofing in the Black Sea: What really happened? - GPS World." Accessed: Apr. 22, 2026. [Online]. Available: <https://web.archive.org/web/20250928103644/https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/>
- [19] J. Burbank, T. Greene, and N. Kaabouch, "Detecting and Mitigating Attacks on GPS Devices," *Sensors*, vol. 24, no. 17, Aug. 2024, <https://doi.org/10.3390/S24175529>.
- [20] D. Ampatzidis, "AIS Spoofing in the Maritime Industry: A Growing Risk and Compliance Challenge." Accessed: Apr. 22, 2026. [Online]. Available: <https://www.marinetraffic.com/ru/maritime-news/34/risk-and%20compliance/2024/11316/ais-spoofing-in-the-maritime-industry-a-growing-risk-and-com>

Energy Security as an Element of National Security

Nikolay Dolchinkov

Vasil Levski National military University, Bulgaria bul.76,
Veliko Tarnovo, 5000, Bulgaria
E-mail: n.dolchinkov@abv.bg,
ORCID: [0000-0002-6171-6083](https://orcid.org/0000-0002-6171-6083)

Abstract—Bulgaria annually consumes about 50 Terawatt hours (TWh) of electricity. Production varies within the same limits. These are the values over the past 5 years. 30–40 years ago, production and consumption were significantly higher, for which there is a historical explanation. In the last century, production and export of electricity were significantly higher, with production significantly exceeding consumption. Bulgaria supplied European Turkey, including Istanbul and Northern Greece. The balance was entirely positive. In the 21st century, electricity production has decreased significantly and since last year a trend for a negative balance of electricity has been observed, i.e. imports exceed exports. By disrupting the balance between production and consumption, Bulgaria becomes dependent on external suppliers and this threatens the country's national security

Keywords — *electricity, production, consumption, energy security, national security.*

I. INTRODUCTION

Energy security is a multi-layered concept that includes reliability of supply, economic accessibility, sustainability and protection of critical infrastructure. In the context of national security, energy security ensures the functioning of state institutions, economic processes, healthcare, transport and defense [1, 2]. Changes in the energy structure, technological transformations and geopolitical upheavals make the topic a strategic priority for state policy. Therefore, energy security is a key element of national security and great attention should be paid to the state of energy and the development trends of the energy sector should be closely monitored both in the region and globally [3], [8], [15].

The methodological approach used in conducting the study was mainly analysis, combining historical retrospection, a systematic review of energy balances (production, consumption, import/export), an assessment of infrastructure vulnerabilities and scenario planning [4], [12], [23]. The report uses available national data, general

principles of energy policy and good practices for risk management [5], [30].

The scope of the study focuses on electricity as a key component of energy security, including consideration of the transmission and distribution network, energy sources (nuclear, coal, gas, renewables), energy markets and strategic reserves; political and operational measures for a 5–30 year horizon [6], [11], [29].

Historical overview of the energy system

Period of export and industrial peak (mid-20th century – late 20th century): Bulgaria developed industrial production and had surplus electricity, which allowed for export to neighboring regions. This structure was based on large base capacities (coal-fired TPPs, NPPs and other plants) and relatively stable domestic consumption [16].

Transition and restructuring (late 20th century – early 21st century): economic and regulatory changes, modernization needs and environmental requirements lead to the closure or reduction of some capacities. In parallel, renewable sources are developed and the energy structure is changing [10], [20].

Modern period (21st century): reduced generation from traditional baseload sources and increasing share of renewables and nuclear energy in the mix. Recent years show a trend towards decreasing net exports and periodic shifts to net imports, which changes energy independence.

Since the beginning of this century, the majority of countries around the world have been pursuing a policy of limiting harmful greenhouse gas emissions and replacing coal and other polluting power plants with alternative and renewable sources, as well as ecological ones that do not pollute the environment [14], [25]. Unfortunately, many of the leading economic world powers and economically developed countries refuse to comply with international treaties and norms and do not even participate in the implementation of the agreements. The European Union, as

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.192>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

one of the major political players, aims to be one of the world leaders in the fight against climate change and in this regard strives to achieve the goals of the agreement of the Conference of the Parties to the United Nations Framework Convention on Climate Change in Paris, while at the same time providing clean energy throughout the continent. Bulgaria, as a member of the union, adheres to the set norms and even the requirements for us are higher than for the economically more developed countries from the western part of the continent [9], [19], [21]. To fulfill this commitment, the EU has set the following binding climate and energy targets by 2030, namely:

1. Reducing greenhouse gas emissions by at least 40% compared to 1990;
2. Increasing energy efficiency to at least 32.5% , as Bulgaria has a lot to catch up on here;
3. Increasing the share of energy from renewable sources to at least 32% of gross final energy consumption in the EU . Here, an assessment of the energy efficiency of alternative sources should also be made, because a large part of them are energy intensive and the electricity consumed is commensurate with the electricity produced;
4. Ensuring a minimum 15% level of electricity interconnection between Member States. Bulgaria is energy-connected with its neighbors in terms of electricity, but the connections are not at the necessary operational level.

In order to ensure a coordinated and coherent approach across the EU and implement the Energy Union Strategy, each Member State was required to submit to the European Commission a draft of its Integrated National Energy and Climate Plan by 31 December 2018 and its final Integrated Plan by 31.12.2019. Bulgaria, as a Member State of the European Union, promptly prepared and submitted to the European Commission its Integrated National Energy and Climate Plan (INPEC) [13], [22].

II. RESEARCH METHODS

Energy balance: annual consumption around 50 TWh; production in the same order, but with visible fluctuations and seasonal deficits. The latest data show periods in which imports exceed exports. This is a trend since 2025, which is deepening with the problems observed in the operation of unit 6 of the Kozloduy NPP and the Maritsa TPP - East.

Generation structure: a combination of nuclear capacity, coal-fired plants (decreasing share), gas-fired capacities and renewable sources (wind, solar, hydro). The dynamics of each component affects the flexibility and stability of the system [7], [18], [26].

Infrastructure: transmission and distribution network with sections that require modernization for the integration of decentralized sources and peak load management. The lack of sufficient energy storage limits the possibility of compensating for the variability of RES.

Risk and vulnerability analysis

1. Geopolitical and market risks

- Import dependence: increases the possibility of price shocks, disruptions and political pressure.

- Volatility of international markets: fluctuations in fuel and electricity prices affect economic stability.

2. Infrastructure vulnerabilities

- Outdated grid: risk of local and systemic failures during extreme loads.

- Insufficient storage: lack of large-scale battery or other storage solutions limits the possibility of flexibility.

3. Technological and operational risks

- Integration of renewable energy sources: without adequate management systems and reserves, the high share of renewable energy sources can lead to instability.

- Cyber risks: digitalization of networks increases exposure to cyberattacks that can paralyze critical systems.

4. Socio-economic risks

- Energy poverty: sharp price increases can affect vulnerable groups and cause social tension.

- Economic vulnerability: industrial users are sensitive to disruptions and price shocks [17].

The main objectives set out in the Bulgarian INPEC are:

- stimulating low-carbon development of the economy;
- development of competitive and secure energy;
- reducing dependence on imported fuels and energy;
- ensuring affordable energy for all consumers.

National priorities in the field of energy can be summarized as follows:

- increasing energy security and diversification of energy resource supplies;
- development of an integrated and competitive energy market;
- use and development of energy from renewable sources, in accordance with the available resources, the capacity of the networks and national specificities;
- increasing energy efficiency through the development and implementation of new technologies to achieve modern and sustainable energy;
- consumer protection by ensuring fair, transparent and non-discriminatory conditions for the use of energy services [24].

III. RESULTS AND DISCUSSION

The integrated plan is fully compliant with the legislation and the main strategic documents at the European and national level.

2 years have passed since the adoption of the plan, but in the last six months significant changes have occurred in Europe and the world. From the short-sighted policy of many political leaders and the transition from long-term

contracts for the supply of energy carriers to completely exchange supplies, where an important role is played not by producers and consumers, but very often by exchange players, intermediaries and proxies of politicians and large resellers. This led to a complete discrepancy between the set forecast prices and the current market prices and caused instability in the energy market and a significant increase in prices. In Bulgaria there are many actions that remain hidden from the public and generally accepted rules are circumvented, leaving great doubts about dirty deals [27].

The electricity market in the Republic of Bulgaria is characterized as national and is played by producers, energy companies, electricity transmission companies, consumers and clients of various caliber. Its structure and organization are regulated by the Rules for Electricity Trading in the Republic of Bulgaria. The electricity market consists of an electricity market through bilateral contracts concluded on the platform of the exchange operator, an exchange market, a balancing energy market, a reserve and additional services market, and a market for the provision of interconnection capacity.

The Bulgarian electricity transmission network is part of the unified transmission network of the countries of continental Europe and its development is closely linked to the development of the networks of neighboring countries. From the reports of the Bulgarian National Energy Exchange, we can note that the total physical imported quantity traded in Bulgaria in 2018 amounted to 2.2 million MWh, 94% of which originated in Romania. The total physical export for the same period amounted to 10 million MWh, distributed: Serbia (23%), Republic of North Macedonia (23%), Greece (21%), Turkey (21%) and Romania (12%). This shows that Bulgaria is predominantly an exporter of electricity to all neighboring Balkan countries. During different days on the exchange market, the distribution is not uniform, with the main influence being the weather conditions, the consumers and producers included in the energy system, the load on the energy system and the requests for electricity supply from neighboring countries. Bulgaria still meets the region's electricity needs, but for example, when one of the Kozloduy NPP units is shut down for recharging, its lack is immediately felt and with increased electricity consumption, the energy systems are put under serious threat. The structure of Bulgaria's electricity sector is such that the Kozloduy NPP and thermal power plants from its own energy sources ensure the balance of consumption (90% of consumption), thermal power plants with imported energy sources work for the additional load, and hydroelectric power plants with 2.7 MWh provide the peak load. In the last decade, many hydroelectric power plants were built not in the right place, and others were shut down that were necessary for our energy sector and proven over time, such as the Chaira hydroelectric power plant, the Belmeken-Sestrimo cascade and others. This was done piecemeal and was not energy-related on a national scale.

Threat	Impact	Likelihood	Priority mitigation
Import dependence	Energy and economic shocks	High	Supply diversification
Reduced production	Loss of energy sovereignty	Medium	Investments in renewable energy and storage
Outdated network	Local and systemic accidents	High	Modernization and digitalization
Regulatory uncertainty	Delayed investments	Medium	National strategy and incentives

Impact on national security

Functional impact: energy supply disruptions affect critical state functions — communications, healthcare, transportation, water supply, and defense capabilities. Political impact: energy dependence can limit foreign policy autonomy and increase vulnerability to external pressures. Economic impact: unstable energy markets and high prices reduce competitiveness and investment attractiveness [28].

Need for a national strategy: a clear, long-term energy strategy with a horizon of 2030–2050, defining priorities, investment mechanisms and regulatory incentives. Market regulation: mechanisms to protect against speculative price shocks, incentives for long-term contracts and mechanisms for strategic reserves. Compatibility with European policies: coordination with regional initiatives, participation in common markets and use of European funds for modernization.

Strategic goals and priorities

1. Restoring energy autonomy by increasing domestic production and diversifying sources.
2. Increasing system flexibility through energy storage, backup capacity and smart grids.
3. Strengthening sustainability through energy efficiency, decarbonization and the development of low-carbon technologies.
4. Protecting critical infrastructure and enhancing cybersecurity.
5. Social justice through measures to protect vulnerable consumers from price shocks.

Operational measures and recommendations

Short-term (1–3 years)

- Adoption of a national energy strategy with specific goals and indicators.
- Creating strategic reserves for critical periods and rapid activation mechanisms.
- Improving energy efficiency in the public sector and key industries.
- Strengthening the cyber defense of energy operators.

TABLE 1 COMPARISON OF THREATS AND MEASURES

Medium-term (3–10 years)

- Investments in energy storage (batteries, hydrogen solutions, compressed air) to compensate for the variability of renewable energy sources.
- Modernization of the transmission and distribution network and implementation of demand management systems.
- Diversification of supplies through regional contracts and interconnections.

Long-term (10–30 years)

- Development of low-carbon baseload capacities and technological solutions for sustainable production.
- Integration of hydrogen technologies and other forms of energy transfer and storage.
- Complete digitalization and automation of network management with a high level of cyber protection.

Implementation plan and institutional coordination

Coordination structure: creation of an inter-sectoral body for energy security, including representatives of ministries (energy, economy, internal affairs, defense), regulator, operators and scientific institutes. Implementation phases: planning and regulatory framework (0–1 year); pilot projects and initial investments (1–3 years); large-scale investments and integration (3–10 years); full transformation and sustainable management (10+ years). Responsibilities: clear division of roles between state authorities, operators and private investors; accountability and control mechanisms.

Expansion of operational measures: I propose a detailed plan in three stages — short-term, medium-term and long-term — with specific actions, responsibilities, indicators and budgetary guidelines for implementation.

Operational stages

Short-term measures 0–18 months

Objective: rapidly strengthen resilience and crisis preparedness. Key actions: adopt a national energy strategy and operational protocols; create strategic reserves and mechanisms for their activation; conduct a national audit of critical energy infrastructure; introduce temporary measures to protect vulnerable consumers; strengthen cyber protection of operators. Responsibilities: Ministry of Energy, State Energy and Water Regulatory Commission, transmission and distribution operators. Key indicators: adopted strategic document; available reserve capacities (MW); priority supply plan. The national strategy and integrated plan documents have already been developed in a framework and serve as a basis for action.

Medium-term measures 1.5–7 years

Objective: increasing flexibility and reducing import dependency. Key actions: large-scale investments in energy storage (batteries, hydrogen solutions); modernization of the transmission and distribution network; deployment of demand management systems and smart grids; incentives for local production and energy

efficiency in industry. Responsibilities: state funds, public-private partnerships, EU funds and banks. Key indicators: installed storage capacity (MWh); percentage of routes with smart devices; reduction of net imports. National plans foresee these priorities as part of the integrated approach.

Long-term measures 7–30 years

Goal: full transformation towards a sustainable, low-carbon and resilient energy sector. Key actions: development of low-carbon baseload capacities; integration of hydrogen economy; regional energy integration and diversification of supplies; full digitalization and automation of management with a high level of cyber protection. Responsibilities: national and regional institutions, industry, research centers. Key indicators: share of low-carbon sources; hydrogen storage capacity; recovery time after an incident.

TABLE 2: COMPARISON OF STAGES

Stage	Time horizon	Basic measures	Key indicator	Priority
Short-term	0–18 months	Strategy; reserves; cyber defense	Plan adopted; reserve capacity	Very high
Medium-term	1.5–7 years	Storage; network modernization	MWh storage; smart routes	High
Long-term	7–30 years	Hydrogen; low carbon bases	Share of low-carbon sources	Medium/High

Most of the transactions are carried out on the “Centralized Market for Bilateral Contracts” segment, which has significantly increased since 2018. The volumes of the “Day Ahead” segment also increased by 43% year-on-year. Also, trading on the “In-Day” segment started in April 2018. Not all neighboring countries have such segments yet. In my opinion, the elimination of medium-term and long-term contracts is a mistake, which does not allow planning the operation of energy capacities and their load and achieving predictable prices, rather than spontaneous price changes caused by stock market speculators.

The price of electricity has also changed significantly in the last few months and instead of the values set in the integrated plan, they now significantly exceed even those set for 2030. The set values were up to 95 €/MWh by 2030 and 106 €/MWh by 2040, however, in October of this year, the exchange prices exceeded 300 €/MWh. This will lead to the need for a complete revision of short-term and long-term programs and has already led to chaos in consumption and large overspending by producers. These high prices, in my opinion, are also the result of the short-sighted policy pursued by the European Union and the leaders of many of the major economic and political countries and unions. This is due to the fact that the market and prices in Europe are unified and the burden on households is different and their economic status is very different in different parts of the European continent. Rich countries, which also have higher incomes, have even lower energy prices than Eastern European countries, which have lower incomes for their

residents. This leads to impoverishment of the population and difficulties in servicing payments for consumed electricity by both household subscribers and industrial enterprises.

This is a problem not only for Bulgaria, but also for many countries in Europe and the world. Even China is currently experiencing a shortage of electricity and some industrial enterprises are operating on a significantly reduced production schedule.

The electricity produced in Bulgaria can be grouped into several main groups: from hydroelectric power plants, thermal power plants, nuclear power, wind generators and photovoltaics. Bulgaria has been and still is a gross exporter of electricity, but the conditions set by the European Commission and the actions of our politicians may soon turn Bulgaria into an importer and thus the national and energy security of the country will depend on other countries.

Bulgaria uses the existing potential of local resources to the maximum extent while complying with environmental requirements. The main energy carriers for energy production are solid fuels in the Maritsa Basin and the nuclear power plant.

Power plants using local coal currently provide about 48% of electricity production and are a guarantor of Bulgaria's energy security and the competitiveness of the Bulgarian economy. Bulgaria will use to the maximum extent the existing potential of local coal in the country while complying with environmental requirements, as they can provide a resource for electricity production for the next 60 years. Here it is planned to reduce the relative share by 2040 to about 3-4% of total electricity production.

Nuclear energy is an important energy carrier that guarantees basic electricity production with predictable and competitive prices. Kozloduy NPP EAD provides over 33% of electricity production in the country and is a guarantor of Bulgaria's energy security. According to the plan, the share of energy from nuclear power plants is expected to increase to almost 60% by 2040, with the net value doubling from 15 GWh to almost 31 GWh.

The use of energy from renewable sources is the third most important local energy resource, which has been increasing in recent years. The main contribution to this is the increased consumption of biomass, as well as the use of solar and wind energy for the production of electricity. The integrated plan provides for an increase in the share of electricity production from wind generators, biomass and solar panels. Over the past 4-5 years, numerous scandals have arisen in Bulgaria related to the unregulated import, storage and incineration of waste from Western European countries, and most of all from Italy. Among the waste there was also very dangerous and toxic waste, which significantly pollutes the environment.

When Bulgaria joined the European Union, we were forced to close the first 4 units of the Kozloduy NPP, each with a capacity of 440 MWh. At this stage, these power units are irretrievably destroyed and cannot be restored.

Over the years, we purchased and subsequently resold 2 VVER 1000 units for the Belene NPP. After arbitration, we purchased another 2 similar third-generation units, which have been unpacked for 3 years now, instead of being used. There is talk of building new capacities at the Kozloduy NPP, fuel diversification, and others, but this is in the realm of talk and political pressure and lobbying for certain companies that do not have the necessary experience and are compromised in the Czech Republic, Ukraine, the Philippines, and other countries.

Upon entering the EU, Slovakia, for example, was also forced to close some of its units, but after 2-3 months it reopened them and did not agree to the conditions set for closure.

In the last 10 days, the European Commission has changed its position on nuclear energy and its chairman, Jan Timmerman, personally said that if we want, we can develop our nuclear energy with new units in Kozloduy, and why not the construction of the power plant in Belene. 10 EU countries, including France, Bulgaria and others, have submitted a document for the continuation of the development of nuclear energy in the European Community. Nuclear energy does not produce greenhouse gases and does not pollute the environment, and with the development of technologies, it is much safer and does not generate waste, unlike some of the green energies.

The US has an appetite for supplying mobile nuclear power plants with small and medium capacity to the countries of Eastern Europe, but this is not a good solution, firstly because these plants have not yet been constructed and secondly, it is not a good solution to deploy numerous small nuclear power plants, which are a potential risk and target of the numerous terrorist attacks that are taking place around the world. It was precisely to lobby for such plants that the US Secretary of Energy visited Central and Eastern Europe in early October.

Bulgaria failed in the years of transition to sufficiently protect its energy and national security with the closure of units 1-4 of the Kozloduy NPP, the agreement on the premature closure of the TPP in the coming years, instead of the conditions achieved by Poland for the operation and subsidization of these plants. After numerous unsuccessful negotiations and the lack of negotiations, the Belene project did not move forward, despite the presence of 2 modern 3+ generation power units at the plant. At the same time, Romania and Turkey are building new nuclear power plants and will thus fill the niche in the energy market in the region. Omissions were made and it is time for politicians to stop serving foreign interests and to protect Bulgarian interests for the development of Bulgarian society.

Risk management and budget guidelines

- Risks: delays in regulatory decisions, lack of funding, technological barriers, social resistance.
- Mitigating measures: phased financing through EU funds and PPPs; pilot projects; communication campaigns for public support.

- Budgetary guidelines: short-term measures - state and operational costs; medium-term - investments in storage and network (hundreds of millions of euros); long-term - billions of euros, distributed in phases and with European co-financing. National documents outline funding opportunities and priorities.

Well make a detailed operational plan

Detailed operational plan for the first 24 months to strengthen energy security

This operational plan describes specific actions, responsibilities, timelines, expected results, indicative budgets and key performance indicators (KPIs) for the first 24 months of the launch of a national program to enhance energy security.

Summary of goals for 24 months

- Ensuring operational strategic reserves and rapid activation mechanisms.
- Launching pilot projects for energy storage and demand management.
- Accelerated modernization of critical sections of the network and increased cyber defense.
- Establishing institutional coordination and a regulatory framework for long-term investments.
- Communication and social protection for vulnerable consumers.

Organizational structure and responsibilities

- National Energy Security Coordination Council — leading coordination and decision-making body.
- Ministry of Energy — operational manager of the program.
- Transmission System Operator (ESO) — technical implementation of network measures.
- Regulator (SEWR or relevant authority) — regulatory changes and monitoring.
- Crisis Management Agency — integration of emergency supply plans.
- Public-private partnerships and financial institutions — financing and implementation of investments.
- Scientific institutes and universities — technical expertise and evaluation of pilot projects.

TABLE 3: SCHEDULE AND KEY ACTIVITIES BY PHASE

Period	Main activities	Responsible	Key result	Indicative budget
Month 0–3	Establishment of a coordination council; adoption of an operational plan; national infrastructure audit	Ministry of Energy; operators	Founding Board; audit report	€0.5–1M

Period	Main activities	Responsible	Key result	Indicative budget
Month 3–6	Creation of strategic reserves; development of crisis protocols; cybersecurity assessment	Crisis Management Agency; operators	Backup plan; cyber assessment	€5–15M
Month 6–12	Launch of 2 pilot battery storage projects; modernization of 2 critical grid sections; energy efficiency program	PPP; ESO; municipalities	50–100 MWh storage; modern routes	€50–150M
Month 12–18	Deployment of demand management systems; training and simulations for crisis scenarios; social measures	Operators; ministries; NGOs	DSR system; exercises conducted	€10–30M
Month 18–24	Evaluation of pilots; scaling up successful solutions; preparation of investment packages for 3–7 years	Ministry; financial partners	Scaling plan; investment proposals	€20–100M

IV. CONCLUSIONS

Here I develop the four conclusions you have indicated, providing for each justification, risks, specific recommendations for action, key responsible institutions, indicative time horizon and indicators of success.

A. Extending the operational life of thermal power plants and developing nuclear energy in Kozloduy and Belene

Maintaining and extending the operational capacity of existing thermal power plants provides baseload capacity and reserve capacity in the transition period to low-carbon energy.

New nuclear capacities increase energy autonomy and provide a large amount of low-carbon electricity, which is important for energy security and climate goals.

Risks:

1. Technical and environmental challenges in extending the life of old capacities.

2. High capital costs and long terms for building new nuclear units.

3. Social and political opposition, as well as regulatory requirements.

Recommendations for action

1. Conduct independent technical assessments of the condition of key TPPs and determine safe terms for extending their operation.

2. Develop an integrated nuclear development plan, including Kozloduy (new units) and Belene (reactivation/completion), with clear financial, regulatory and environmental criteria.

3. Financial planning: combining state funds, European co-financing and private investments; assess public-private partnership models.

4. Transparent public consultations and communication program on safety, economic benefits and environmental measures.

Responsible institutions: Ministry of Energy; Nuclear Regulatory Agency; plant operators; international experts.

Time horizon:

Short term: 1–3 years for assessments and planning.

Medium term: 3–10 years for life extension and initial construction activities.

Long term: 10+ years for full implementation of new nuclear capacities.

B. The European context and requirements for third generation nuclear reactors

The European institutions set high standards for safety and cost-effectiveness for new nuclear projects. Compliance with these standards is a prerequisite for access to financing, insurance and public trust.

Risks

1. Failure to comply with the requirements may lead to the rejection of European co-financing, difficulties in licensing and increased costs.

2. Choosing obsolete or incompatible technologies increases operational and environmental risks.

Recommendations for action

1. Requirement of third generation or equivalent safety technologies for all new nuclear projects.

2. Assessment of technological options through international expertise and comparative cost-benefit analyses.

3. Integration of best practices in safety, waste management and emergency procedures.

Responsible institutions: Ministry of Energy; Nuclear Regulatory Agency; international consultants; European funds.

C. Delays, administrative procedures and increasing costs for energy projects

Numerous committees, lengthy expert assessments and complex procedures increase the time for implementation and the final price of projects. This leads to a greater financial burden on the state and taxpayers.

Risks

1. Loss of investor interest; increased project costs; dependence on expensive external analyses and consultants.

2. Negative effect on competitiveness and the ability to respond quickly to energy crises.

Recommendations for action

1. Procedural reforms: optimization and digitalization of administrative processes; introduction of clear deadlines for consideration and decisions.

2. Establishing fast-tracks for strategic projects with guarantees of transparency and control.

3. Developing national expert capacity through training and cooperation with academic centers to reduce dependence on expensive foreign analyses.

4. Cost control mechanisms: standardized contracts, transparent tenders and performance monitoring.

Responsible institutions: Ministry of Energy; Council of Ministers; regulatory authorities; Public Procurement Agency.

Time horizon:

Short-term: 6–18 months for procedural changes and digitalization.

Medium-term: 1–4 years for building national expert capacity.

Success indicators

D. Need for a strategic investor in protecting national interests

Large energy projects require significant investments and long-term partnerships. A strategic investor can provide capital, technology and operational expertise. At the same time, national interests must be protected through clear conditions and control mechanisms.

Risks: Entry of investors with interests that do not coincide with national priorities; loss of control over critical infrastructure; possible political and economic dependencies.

Recommendations for action

1. Define criteria for a strategic investor: technological capacity, financial health, experience in nuclear energy, commitment to the local economy and compliance with national regulations.

2. Mechanisms to protect the national interest: retention of a state share or special rights (golden shares) in key projects; clauses for technology transfer and localization of production; clear conditions for management and control.

3. Transparent selection procedures with international tenders, evaluation of offers according to security and public interest criteria.

4.Commitment to long-term partnership: guarantees for investments in training, infrastructure and local value chains.

Responsible institutions: Ministry of Energy; Ministry of Finance; Government Commission for the Selection of Strategic Investors; Regulator.

Time horizon:

Medium term: 1–3 years for selection and conclusion of agreements.

Long term: implementation and monitoring throughout the project life cycle.

Establish a cross-sectoral monitoring mechanism with public reports every 6 months and independent audit of progress.

REFERENCES

- [1] Dolchinkov N., History, development and prospects of the Belene NPP project, Scientific conference "Radiation safety in the modern world", National University "V. Levski", Veliko Tarnovo - November 11, 2016. ISBN 978-954-753-243-4 pp. 81-90;
- [2] Dolchinkov N., B. Karaivanova-Dolchinkova, The role of nuclear energy in the world economy, Scientific Conference "Radiation Safety in the Modern World", National University "V. Levski", city of Veliko Tarnovo - November 20, 2020. ISSN 2738-7607 Print, ISSN 2603-4689 CD, pp. 250-260;
- [3] Manchev B., Belene NPP – lectures before the Energetik club, Sofia, 2010;
- [4] Nabatov N. and colleagues, The Electric Power Industry of Bulgaria, TANGRA TanNakRa IC, Sofia, 2015;
- [5] Decrees and decisions of the Council of Ministers of the Republic of Bulgaria, Sofia [Accessed: Feb. 13, 2026].
- [6] Haralampiev M., The Development of Nuclear Energy and Nuclear Arsenals, Collection of Reports from the Scientific Conference "Current Issues of Security " , volume 6, Publishing Complex of the National University "Vasil Levski " , 2020, pp. 123-133, ISSN 2367-7475;
- [7] Council of Ministers of the Republic of Bulgaria, Integrated Plan in the Field of Energy and Climate of the Republic of Bulgaria 2021 - 2030, Sofia 2020;
- [8] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Improvement of Constructive-Technological Approaches Reducing Innovative Obsolescence of Industrial Technologies in the Context of Industry 4.0, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 180–186.
- [9] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Study of the State of Innovation Development and Obsolescence in the Republic of Bulgaria of Companies from the Mechanical Engineering Sector, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 187–194.
- [10] Petrova, D., Innovative Obsolescence in Mechanical Engineering and Singleness of Indicators, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2024, 3, pp. 221–224.
- [11] Toneva, D., Dimitrova, D., Some aspects of the water crisis in Bulgaria, 5th International Scientific Practical Conference „Environment. Technology. Resources “, Published by Rezekne Academy of Technologies, Latvia. Volume I, pp. 373-377, ISSN 1691-5402, ISBN 978–171389957–0.
- [12] Rachovski, T., Petrova, D., Ivanov, I., Automated Creation of Educational Questions: Analysis of Artificial Intelligence Technologies and Their Role in Education, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2024, 2, pp. 465–467.
- [13] Petrova, D., An Approach to Modeling Innovation Obsolescence, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 175–179.
- [14] Loktionov, O.A., Fedotova, E.V., Kondrateva, O.E., Dolchinkov, N.T., Kuznetsov, N.S. Actual and design wind loads for overhead transmission lines in the Central European part of Russia, IOP Conference Series: Earth and Environmental Science This link is disabled., 2023, 1281(1), 012050
- [15] L. Poiša, L. Antypova, Evaluation of the Effects of Herbicides on the Weeds and the Productivity of Hybrids Maize. Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 14 th International Scientific and Practical Conference, vol. 1, pp. 195–199, Jun. 2023, doi: 10.17770/etr2023vol1.7204.
- [16] Stanchev G., Technical obstacles to speech intelligibility, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 3, pp 300-305
- [17] Simeonov M., M. Marinov, Determine the location of nodes in wireless sensor network by using genetic algorithm, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 2, <https://doi.org/10.17770/etr2024vol2.8059> pp 247-252
- [18] V. Vasilev, D. Stefanova, and M. Icheva (2024). Green human resource management as a component of sustainable organizational development in environmental and natural economics, ETR, vol. 1, pp. 402–407, Jun. 2024, doi: 10.17770/etr2024vol1.7966
- [19] Bulatom. (2022). Nuclear Energy - The Basis for Sustainable Development. <https://www.bulatom-bg.org/> [Accessed: Feb. 13, 2026].
- [20] Council of Ministers of the Republic of Bulgaria. (2020). Integrated Plan in the Field of Energy and Climate of the Republic of Bulgaria 2021 – 2030. Author. [Accessed: Feb. 13, 2026].
- [21] Council of Ministers of the Republic of Bulgaria. (2019). Resolutions and decisions of the Council of Ministers of the Republic of Bulgaria, Sofia. Author. [Accessed: Feb. 23, 2026].
- [22] Dolchinkov, N., & Karaivanova-Dolchinkova, B. (2021). Modern plans for development of production of electricity worldwide and energy independence of Bulgaria, Scientific conference “Radiation safety in the modern world”, NSU “V. Levski”, 392-399.
- [23] Haralampiev, M. (2020). The development of atomic energy and nuclear arsenals. Collection of reports from the Scientific Conference “Current Security Issues”, 6, 123-133.
- [24] IAEA. (2023, May 1). International Atomic Energy Agency. <https://www.iaea.org/> [Accessed: Feb. 23, 2026].
- [25] Kozloduy NPP. (2023, May 10). Kozloduy Nuclear Power Plant. <https://kznpp.org/> [Accessed: Feb. 23, 2026].
- [26] Dolchinkov N., Optimizing Energy Efficiency in the Conditions of a Global Energy Crisis, Optimizing Energy Efficiency During a Global Energy Crisis, IGI Global, ISBN13: 9798369304006|ISBN13 Softcover: 9798369304044|EISBN13: 9798369304013, DOI: <https://doi.org/10.4018/979-8-3693-0400-6>

Research on the Effects of Specific Radionuclides on Health

Nikolay Dolchinkov

Vasil Levski National military University, Bulgaria bul.76,
Veliko Tarnovo, 5000, Bulgaria
E-mail: n.dolchinkov@abv.bg,
ORCID: [0000-0002-6171-6083](https://orcid.org/0000-0002-6171-6083)

Abstract: Radionuclides affect human health and living organisms through external and internal exposure. This causes acute effects at high doses and an increased risk of cancer and genetic damage at long-term low-level exposure. Radionuclides generally affect health, toxicology and public health through chemical and radiation effects - internal uptake (ingestion/inhalation) of specific isotopes such as I-131, Cs-137 and Sr-90 leads to local accumulation in critical organs and an increased risk of cancer and functional disorders. The main routes of entry of hazardous radionuclides into the human body are through air, water, food and injured surfaces. It is very important to conduct radiation reconnaissance of the isotopes distributed in the environment and their energy state. Public health protection responds to the presence or change in the composition of radionuclides through monitoring, dietary restrictions and protective measures (evacuation, iodine prophylaxis). Radionuclides have a combined effect, causing on the one hand a radiation component (ionizing damage to DNA) and on the other hand a chemical/toxicological component (for example, heavy metals such as uranium have nephrotoxicity).

Keywords: radiotoxicology, air, soil, water, food, radionuclides, uranium, strontium, iodine, cesium, human organism, impact, organs, tissues, impact.

I. INTRODUCTION

Radionuclides are unstable atomic nuclei that release ionizing radiation through radioactive decay and interact with biological systems in ways that carry important public health consequences [1, 6, 12]. This chapter explores the multifaceted effects of radionuclides on population health by integrating physical, ecological, and epidemiological viewpoints. Its purpose is to offer a systematic overview of the issue, outline the methods used for assessment and surveillance, review empirical findings, and draw practical conclusions and recommendations relevant at the national level as well as for local hotspots such as the Veliko Tarnovo region [2], [35], [46], [50].

Radionuclides—both natural (uranium, thorium, radon) and anthropogenic (cesium-137, strontium-90, NORM/TENORM)—are inherent components of the geochemical environment and an unavoidable part of our surroundings [2], [11], [21], [37]. Their potential hazard to human health and ecosystems depends on concentration, origin, energy released, and exposure pathway [10]. In Bulgaria, uranium deposits, former uranium mines, certain industrial sites, and local geological conditions create the potential for localized hotspots that require focused monitoring and management [3], [18], [22], [41], [44]. Monitoring efforts have been conducted in the past, notably under the PHARE programme at the end of the 20th century and by Plovdiv University in 2010, but periodic re-surveys are necessary because radionuclide distributions change over time and ongoing surveillance is required.

The primary aim of this study is to establish a scientifically robust framework for understanding sources and mechanisms of radionuclide exposure [33], [39]. To that end, the chapter describes monitoring and assessment techniques, proposes a structure for an operational protocol for local surveys, and offers practical and legislative recommendations to reduce risk [8], [29], [36], [42], [48].

II. RESEARCH METHODS

To achieve the set goals, the following have found a place in the structure of the article:

- historical and regulatory context of the issue under consideration;
- describing sources and routes of exposure to the main radionuclides;
- biological mechanisms of radionuclides' impact on living organisms;
- methodology for monitoring the presence of radionuclides in air, water and soil;

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.195>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

- epidemiological approaches to detecting the presence of certain radionuclides [15], [25];
- operational protocol for sampling and reporting based on the Veliko Tarnovo district;
- risk assessment in the event of the possible detection of radionuclides;
- remediation [16], [28], [43];
- legislative and communication measures aimed at limiting the possibilities for the release of radionuclides and limiting their impact on the environment;
- methodological appendix and extended tables.

Historical and regulatory context:

Purpose: Trace the development of scientific knowledge, policy, and the regulatory framework that shape radionuclide management.

Content: A timeline of key events; review of national and European legislation and standards for permissible levels and control methods; evaluation of past monitoring programmes and their outcomes; identification of regulatory gaps and proposals for updates [4], [14].

Sources and exposure pathways:

Purpose: Describe the main natural and anthropogenic sources and the routes by which people and ecosystems are exposed.

Content: Classification of sources such as geological deposits, mining, industrial sites, nuclear incidents, and agricultural technologies; transmission pathways including air, water, soil, and food; factors affecting mobility and bioavailability; exposure scenarios for different population groups including workers, local communities, and vulnerable subpopulations [5], [38].

Biological mechanisms of impact:

Purpose: Explain how ionizing radiation and specific radionuclides interact with biological systems.

Content: Physicochemical properties that determine biological behavior; cellular and molecular damage mechanisms such as DNA lesions and oxidative stress; distinctions between external and internal exposure; dose-response relationships and latency periods; organ- and age-specific vulnerabilities [13], [31], [40].

Monitoring methodology for air water and soil:

Purpose: Present practical, scientifically grounded methods for detecting and quantifying radionuclides.

Content: Selection of indicator samples and matrices; sampling strategies including locations, depths, and sample volumes/masses; analytical techniques such as gamma spectrometry, alpha/beta counting, and mass spectrometry; detection limits; quality control and calibration procedures; monitoring frequency and alarm criteria [7].

Epidemiological approaches to detecting health effects:

Purpose: Describe study designs and analytical methods used to link exposure to health outcomes.

Content: Study types including ecological, cohort, and case-control designs; individual exposure assessment and use of biomarkers; adjustment for confounders; statistical methods for assessing associations and causality; interpretation of findings and study limitations [49].

Operational sampling and reporting protocol for Veliko Tarnovo district:

Purpose: Provide a concrete, actionable procedure for local surveys and rapid response.

Content: Sampling plan with mapped sampling points and priority zones such as former mines, industrial sites, and water sources; sample types including soil layers 0–10 cm and 10–30 cm, surface and groundwater, air filters, and foodstuffs; sampling frequency covering baseline surveys, seasonal repeats, and post-incident sampling; required analytical methods and laboratory standards; quality assurance measures including replicates, blind samples, and reference materials; alarm thresholds and response steps such as resampling and expanded investigations; report format with standardized tables, geospatial maps, and layperson summaries; communication procedures for notifying local authorities, health services, and the public.

Risk assessment following radionuclide detection:

Purpose: Provide a framework for quantitative and qualitative risk evaluation to support decision making.

Content: Dose assessment models for internal and external exposure; conversion of measured concentrations into expected doses for defined scenarios; use of health risk thresholds; sensitivity and uncertainty analysis; prioritization of interventions based on risk-benefit considerations [19], [27].

Remediation and exposure reduction measures:

Purpose: Describe technical and managerial options to limit impact and reduce exposure.

Content: Short-term measures such as access restrictions, dust control, and water filtration; long-term remediation technologies including excavation and secure disposal, stabilization, and bioremediation; evaluation of effectiveness and costs; post-remediation monitoring requirements; recommendations for priority actions in the local context [20], [45].

Legislative and communication measures:

Purpose: Propose policies and strategies for prevention, control, and public information.

Content: Suggested regulatory updates and standards; institutional coordination mechanisms; crisis communication plans; community education campaigns; transparency measures and stakeholder engagement processes [23].

Methodological appendix and extended tables:

Purpose: Provide technical details and supporting data that underpin the main text.

Content: Detailed sampling and analytical protocols; report templates; tables of reference values and detection limits; worked examples for dose calculations; inventory of equipment and suppliers; supplementary maps and charts.

Uranium, thorium and other radioactive families are part of the earth's crust [4], [13], [17]. Their distribution depends on the geological history and lithology of specific regions [5], [20], [47]. In areas with granitic and metamorphic rocks, a high radon potential is often observed. The largest reserves of uranium ores are in Kazakhstan, Canada, Australia, Nigeria and other countries, with the first 3 countries owning more than 60% of the world's deposits. Bulgaria also has uranium deposits, mainly located in the Rila-Rhodope mountain system, the Central part of the Thracian Lowland and the Stara Planina. Uranium was mined in Bulgaria from 1939 to 1991, when by decision of the Council of Ministers of the Republic of Bulgaria, uranium mining was stopped and all uranium deposits were preserved. In Bulgaria, there were 2 uranium processing plants located in the town of Buhovo 1 near Sofia, and in the village of Eleshnitsa (near Razlog). Currently, these plants are closed. Bulgaria is perhaps the only country that has uranium deposits but does not exploit them. Currently, the largest uranium extraction is carried out in Kazakhstan.

Anthropogenic sources are mainly related to mining activities (uranium mining), mineral processing, industrial processes, use of materials with naturally elevated radionuclide content (NORM/TENORM), as well as historical deposits from nuclear tests and accidents [7], [19], [34]. They are the causes of local increases in radionuclides in soils, sediments and waters. In Bulgaria, uranium mining mines and enterprises have been closed since 1991, but the situation around them is monitored because there are underground rivers whose waters pass through uranium deposits and mines, winds raise dust from the tailings ponds of the closed enterprises in Buhovo and Eleshnitsa and increase the content of radionuclides in the air. On several occasions in Haskovo and other settlements, an increased content of uranium in drinking water was detected, which is determined by the origin of groundwater and leads to restrictions on the use of water sources for drinking purposes. It should not be overlooked that all mineral waters contain a certain amount of radioactive isotopes [8], [14], [32].

As a general statement for Bulgaria, it can be stated that uranium mining was active from 1939 to 1991, with the main areas being along the Rhodope Mountains from Asenovgrad in front of Smolyan to Razlog at the foot of Pirin, the Central part of the Thracian Lowland in the Plovdiv region, the Stara Planina in the Chiprovtsi region, the Iskar Gorge and the Sliven region as a potential but not operating at this stage. The tailings ponds of the uranium processing plants in the Buhovo and Eleshnitsa regions with the available mining waste and some industrial sites in these regions have been documented as potential sources of local pollution. The presence of geological zones with increased radon potential (e.g. areas with granites and metamorphic rocks) such as the Rhodope Mountains, Pirin,

the Sofia Plain, the Central Thracian Lowland and others makes a local assessment necessary in these regions.

III. RESULTS AND DISCUSSION

3.1 Main sources

- Radon (^{222}Rn) is a gaseous product of the decay of uranium. The main source is the soil and rocks under buildings, but it is also often released from materials used for construction such as bricks, sand, gravel [15], [24]. In Bulgaria, a national program for the prevention of radon emissions in public buildings, such as kindergartens, schools, etc. is in operation. There are publications on research conducted. One of the sources is materials used in the production of which were materials from Serbia or produced on the territory of part of the territory of the former Yugoslavia, which were contaminated with radioactive isotopes as a result of the bombing of Serbia in 1999 with bombs containing uranium.
- Uranium (^{238}U , ^{234}U), which is naturally present in soils and rocks in areas with uranium deposits. In Bulgaria, this is mainly the Rila-Rhodope region and the Central part of the Thracian Lowland. It can be dissolved in groundwater and enter water bodies on the earth's surface.
- Radium (^{226}Ra) is a product of the various uranium families. It is characterized by accumulating mainly in sediments and soils.
- Anthropogenic isotopes such as ^{137}Cs , ^{90}Sr , ^{131}I . Their origin is mainly from nuclear tests and accidents. They are characteristic of sediments and biota and have different half-lives [9], [30].
- NORM/TENORM are industrial wastes with a naturally elevated content of radionuclides, such as in the mining and processing industry. This applies not only to the uranium mining industry, but also to the extraction of other raw materials, because ore deposits usually contain a wide variety of chemical elements in different forms, but not all of them are extracted during extraction. This also includes waste from secondary raw materials, which sometimes contain elements with a content of certain low-activity radioisotopes.

TABLE 1 MAIN RADIONUCLIDES, EXPOSURE ROUTES AND KEY EFFECTS

Radionuclide	Exposure routes	Key effects
Rn -222	Inhalation	Lung cancer
^{238}U	Ingestion	Internal irradiation; nephrotoxicity
^{226}Ra	Ingestion; inhalation	Accumulation in bones; bone tumors
^{137}Cs	Ingestion	Internal exposure; accumulation in biota

3.2 Exposure routes

- Inhalation or airborne uptake is the primary route of entry for radon and particulate matter carrying decay products. Gas masks should be used to limit access to the respiratory tract for protection.

- Ingestion of contaminated drinking water (soluble uranium, radium), consumption of fish, fish products and other biota from contaminated water bodies. This also includes consumption of plant products that have been contaminated as a result of a radiation accident. In the event of a radiation accident, food of animal origin from an area contaminated with radioisotopes should not be consumed.

- Direct contact with contaminated soils and sediments during occupational exposures when working with waste, soil treatment, sampling, etc.

3.3 Biological mechanisms

Ionizing radiation, when entering the human or animal body, causes direct (DNA breaks) and indirect (free radical formation) damage. In addition to the short-term or momentary effects that are observed immediately after exposure to radionuclides, long-term effects are also observed, which include an increased risk of malignant diseases (especially lung cancer in the case of radon), bone and kidney effects in the case of accumulation of radium and uranium, as well as potential genetic and reproductive effects at high doses. These effects are very often transmitted genetically to subsequent generations and cause changes at different levels. The chemical toxicity of uranium (non-radiological effect) is important at high concentrations in drinking water and manifests itself primarily as nephrotoxicity. Therefore, one should not overdo the consumption of mineral waters with a high content of radon or other radioactive isotopes and periodic monitoring of mineral water springs and drinking sources should be carried out [26].

The influence of radionuclides should not be overexposed when processing foods with certain radioisotopes in order to increase their durability, storage, and quality.

3.4. Interpretation of results and risk assessment

3.4.1 Mapping and spatial analysis

To begin with, it is necessary to have GIS approaches. It is necessary to do karnography and thus visualize the measured radon values and concentrations of uranium, radium or other isotopes. It is important to use interpolation methods such as kriging for mapping. At the same time, when processing the obtained results, a mathematical analysis of clusters and correlation with geological and hydrological factors should be done. In this way, all factors for the spread of pollution will be taken into account as accurately as possible.

3.4.2 Estimation of annual effective doses

When estimating annual effective doses, an appropriate model for conducting the study should be selected. When collecting data and processing and analyzing them, annual effective doses for inhalation of radon or radon compounds, ingestion through drinking water and contact with soil and other surfaces should be calculated. When performing the assessment, conservative assumptions for exposure time and bioavailability factors should be used. The results obtained should be compared with current national standards and compared with international recommended

thresholds and measured values in nearby areas from neighboring countries.

3.4.3 Criteria for priority interventions in measurements in different environments.

When measuring in homes, public buildings, schools and kindergartens and detecting radon above the specified action threshold, the priority of the actions is remediation. It is necessary to limit access to the buildings and carry out the appropriate activities to reduce the content of radon compounds [30].

When uranium, radium or other radioisotopes are detected in drinking water above permissible levels, it is recommended to apply purification technologies or alternative water supply [31]. In Bulgaria, such cases occurred several times in one of the water sources in Haskovo and adjacent villages, where the use of water from the water supply network was prohibited until the uranium content was normalized. In the Veliko Tarnovo region, there were no such deviations in terms of radioisotopes, but in the summer of 2025 there was a high content of soil particles and the use of drinking water from the water supply network was suspended for 4 months.

When examining soils and sediments from the bottom of water bodies, specific activities that pose a risk of contact or resuspension of sediments are examined. If necessary, multiple samples are taken to determine the area of contamination and the extent of the presence of radioisotopes or other contaminants. The study should continue until the values of the radioisotopes or other contaminants present are within the permissible limits [32].

3.5. Risk management and technical measures

3.5.1 Measures to reduce the content of radon or radon compounds in residential or public buildings, schools and kindergartens.

- 1) Improving ventilation and air movement inside buildings. This can be achieved by using mechanical or passive ventilation, depending on the building design, or a combination of both.

- 2) Sealing joints and foundations to reduce soil gas infiltration. If possible, limit openings to the soil as much as possible so that radon from the earth's crust cannot enter the foundation of the building. There should be a concrete belt around the building to prevent gas from the interior of the earth's crust from coming to the surface in the immediate vicinity of the walls and penetrating the buildings through joints, cracks or other openings in the walls.

- 3) Installation of a radon barrier in new construction. All construction materials must be checked for the presence of radioactive isotopes or their compounds upon arrival at the construction site and if hazardous components are found, they must be returned to the supplier and not used in construction. At each stage of construction, control must be carried out of the completed and upcoming materials for use in the construction of the building.

4) To build active drainage systems (sub slab depressurization (SSD)) at high values and continuous follow-up monitoring is performed. This system uses an electric fan to create a pressure gradient in the foundation portion of the building to mitigate the potential for vapor intrusion from the subsoil into the building. The types of fans that can be used for SSD can vary depending on the permeability of the foundation material, as well as the type of building, the quality of construction, and the size of the building.

3.5.2 Purification of water in which radon, uranium, radium or other isotopes have been detected can be carried out in several ways.

1) Reverse osmosis is effective for removing soluble uranium and radium.

2) Ion exchange resins are used in the selective removal of uranium and radium.

3) Centralized solutions for small communities are implemented in packaged systems, water delivery by water carriers, or bottled water delivery.

3.5.3 Remediation of soils and sediments

1) excavation and safe disposal or capping of contaminated areas are most commonly used . In these methods, the top 5-10 cm of topsoil is removed, deposited in a repository at a certain depth, and a new topsoil layer is placed.

2) The second most important procedure is chemical stabilization, which uses additives to reduce the mobility of radionuclides in the contaminated area of the soil surface.

3) Phytoremediation requires a longer period of implementation. It involves the use of plants to extract hazardous radionuclides or stabilize the surface soil layer under appropriate conditions.

4) The priority in carrying out topsoil remediation activities is to resolve the contamination problem as quickly and efficiently as possible. The focus is usually placed on areas with the highest risk and the greatest potential for human exposure.

TABLE 2: POINTS WITH DOCUMENTED ELEVATED/SIGNIFICANT RADIONUCLIDE VALUES IN BULGARIA

N o.	Location	Matrix	Radionuclide(s)	Reported value (units)	Comment / data status
1	National (representative survey)	Indoor air (residential)	Rn -222	Arithmetic mean 111 Bq /m ³ ; GM 81 Bq /m ³ (2778 dwellings , 2015–16)	National survey; shows spatial variability between areas.
2	Buhovo (historic uranium sites)	Soil	238U, 235U, 234U	238U = 2489 Bq / kg ;	Locally highly contaminated

N o.	Location	Matrix	Radionuclide(s)	Reported value (units)	Comment / data status
				235U = 117 Bq / kg ; 234U = 2107 Bq / kg (measured contaminated samples)	tailings pond samples; example of a hot spot.
3	Rilo -Rhodope s (selected mineral springs, Southwestern/ Southern Bulgaria)	Mineral/drinking water	226Ra, 210Pb, U (soluble)	Example s: 226Ra 13–168 mBq /L; U up to ~21 µg /L (variable values in different sources)	Data from regional surveys; values vary by source.
4	Kozloduy (nuclear power plant area, monitoring)	Waters, sediments, soils	137Cs, 90Sr, natural U/ Th	Long-term monitoring; values within control levels, with local variations (annual reports)	Regular annual reports and monitoring; data are public in the operator/supervisory reports.
5	Yovkovtsi Lake (V. Tarnovo, local studies)	Water, sediment, biota	Natural radionuclides (U/ Ra series)	Local spectra and measurements; numerical series are fragmentary in reports	Conference /local reports available ; no centralized public database.
6	Black Sea coast (Varna, Burgas, etc.)	Marine sediments, biota	137Cs, 40K, 226Ra, 232Th, 210Pb	Spatial variability; 137Cs in sediment s traces historical deposits (values from surveys)	Scientific and monitoring studies; values depend on sediment type and local input.
7	Industrial sites (example: Kronoshpan, Veliko Tarnovo)	Soil, dust, air	(mostly non-background emissions; radionuclides not systematic)	Public inspections and temporary shutdowns; no systematic	Targeted radiation sampling around the site is recommended.

N o.	Location	Matrix	Radionucl ide(s)	Reporte d value (units)	Comment / data status
			ally reported)	radiation series	

IV. CONCLUSIONS

Radionuclides constitute a complex environmental and public health challenge that demands a coordinated, multidisciplinary response. Effective management requires the integration of robust scientific monitoring, targeted technical interventions, continuous health surveillance, clear legislative frameworks, and proactive public communication. Each component reinforces the others: monitoring identifies problems and guides remediation; health surveillance detects and quantifies impacts; legislation establishes standards and responsibilities; and transparent communication builds public trust and enables timely protective actions.

Sustained, periodic studies are essential. Radionuclide distributions and exposure pathways change over time due to natural processes, land use, and human activities. Regular re-surveying, data analysis, and public reporting ensure that risk assessments remain current and that hotspots are detected early. For Bulgaria and for regions such as Veliko Tarnovo, priority actions include systematic mapping of radon, uranium, and other radioisotopes in housing, soils, and water sources, together with the establishment of a long-term risk management framework that links monitoring results to concrete mitigation measures.

Capacity building and institutional coordination are critical. Successful implementation depends on trained personnel, accredited laboratories, interoperable data systems, and clear lines of responsibility among national and local authorities, health services, and environmental agencies. Financial support and sustained political commitment are required to maintain monitoring networks, fund remediation, and deliver community outreach and education.

Community engagement and transparency must be central. Clear, timely communication of findings, health implications, and recommended actions empowers residents and stakeholders to participate in risk reduction. Public registers, accessible maps, and plain-language reports increase accountability and facilitate local decision making.

In sum, a proactive, evidence-based programme that combines monitoring, remediation, regulation, health surveillance, and public engagement will reduce exposure, protect public health, and create a resilient framework for managing radionuclide risks at national and regional levels.

Operational Next Steps

1 Launch pilot monitoring and consolidate local data

Scope: Implement pilot radon surveys in representative housing types and targeted water testing at key supply points.

Deliverables: Baseline dataset, standardized sampling protocols, and a centralized database of historical and new measurements.

Timeline: 6–12 months for initial pilot and data consolidation.

Lead: Ministry of Environment in partnership with regional health authorities and accredited laboratories.

2 Create an intermediate working group

Composition: Experts in radiation protection, hydrology, epidemiology, environmental chemistry, and representatives from local government and civil society.

Mandate: Oversee pilot activities, review data quality, advise on sampling expansion, and coordinate stakeholder communication.

Deliverables: Terms of reference, meeting schedule, and interim technical guidance.

Timeline: Establish within 1–2 months of pilot launch.

3 Prepare a national radon map and public register

Scope: Aggregate pilot and historical data to produce a geospatial radon risk map and an open public register of measured values and monitoring sites.

Deliverables: Interactive map, downloadable datasets, and a public portal with explanatory materials.

Timeline: 12–18 months for initial map; ongoing updates thereafter.

Lead: National radiation protection authority with GIS support from academic partners.

4 Develop subsidized remediation and training programmes

Scope: Design financial incentives and technical assistance for radon mitigation in homes, remediation of contaminated sites, and water treatment where needed.

Deliverables: Subsidy schemes, contractor accreditation standards, training curricula for technicians and public health staff, and pilot remediation projects.

Timeline: Policy design and pilot roll-out within 12–24 months.

Lead: Ministries of Health and Environment with local government implementation.

Expected Outcomes and Implementation Considerations

Outcomes: Establishment of a reliable monitoring network; comprehensive regional and national maps of radon and other radioisotopes; evidence-based remediation actions in priority areas; improved public awareness and reduced exposure for vulnerable populations.

Implementation considerations: Secure multi-year funding; ensure laboratory accreditation and quality assurance; adopt interoperable data standards; build local technical capacity; and design communication strategies that are culturally appropriate and accessible.

Funding and governance: The plan requires committed funding streams and a clear governance model that assigns responsibilities for monitoring, data management, remediation, and public communication. Pilot results should be used to refine cost estimates and to mobilize national and international support.

REFERENCES

- [1] International Commission on Radiological Protection . (2010). ICRP Publication 115: Lung cancer risk from radon and progeny and statement on radon . ICRP [Accessed: Feb. 13, 2026].
- [2] United Nations Scientific Committee on the Effects of Atomic Radiation . (2008). Sources and effects of ionizing radiation (UNSCEAR 2008 Report). United Nations [Accessed: Feb. 13, 2026].
- [3] World Health Organization . (2009). WHO handbook on indoor radon : A public health perspective . World Health Organization [Accessed: Feb. 13, 2026].
- [4] European Commission . (2013). Council Directive 2013/59/Euratom laying down basic safety standards for protection against the danger arising from exposure to ionizing radiation . Official Journal of the European Union [Accessed: Feb. 13, 2026].
- [5] Vassilev G., (2005), Radio ecology , Tita consulting , Sofia ;
- [6] Vasilev, V., Stefanova, D., Popescu, C. (2023). Human capital management and digitalization - From good practices and traditions to sustainable development; Book Chapter: Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, pp. 41–65; <https://doi.org/10.1108/978-1-83753-190-520231004>
- [7] Dimitrov B., (2019), Problems in the special preparation for nuclear, chemical and biological protection, Collection of reports from a scientific conference, IV International Scientific Conference High Technologies. Business. Society 11-14.03.2019, Borovets, Bulgaria, Volume Iii "Society", pp. 263-265, ISSN 2535-0005
- [8] Loktionov , OA, Fedotova , EV, Kondratova , OE, Dolchinkov , NT, Kuznetsov , NS (2023), Actual and design wind loads for overhead transmission lines in the Central European part of Russia, IOP Conference Series: Earth and Environmental Science This link is disabled., 2023, 1281(1), 012050
- [9] Dolchinkov N., (2023), Optimizing energy efficiency in the conditions of a global energy crisis, Optimizing Energy Efficiency During a Global Energy Crisis, 2023, ISBN: 9798369304006 EISBN: 9798369304013, <https://doi.org/10.4018/979-8-3693-0400-6> pp . 1–9
- [10] Todorov , DN, (2019), State of the population disclosure systems in the changing radiation situation in Bulgaria , Vide. Technology. Resources - Environment , Technology, Resources , 1, pp . 54–58
- [11] Adamovics A., Poisa L. (2017) Evaluation of chemical content in different energy crops. In: The 8th International scientific conference "Rural development 2017: Bioeconomy Challenges": abstracts book, Kaunas, Lithuania, 23-24th November, 2017 Aleksandras Stulginskis University, Ministry of Agriculture of the Republic of Lithuania - Kaunas, pp. 199.-202.
- [12] V. Vasilev, D. Stefanova, and M. Icheva (2024). Green human resource management as a component of sustainable organizational development in environmental and natural economics, ETR, vol. 1, pp. 402–407, Jun. 2024, <https://doi.org/10.17770/etr2024vol1.7966>
- [13] L. Poiša, L. Antypova , (2023), Evaluation of the Effects of Herbicides on the Weeds and the Productivity of Hybrids Maize . Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 14 th International Scientific and Practical Conference, vol. 1, pp. 195–199, Jun. 2023, <https://doi.org/10.17770/etr2023vol1.7204>.
- [14] N.T. Dolchinkov, N. I. Padarev, Radioactive Waste Storage as an Element of National Security, , Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 81-87, DOI: <https://doi.org/10.17770/etr2025vol5.8502>
- [15] N. I. Padarev, N.T. Dolchinkov, Analysis of a Radiological Incident in Nuclear Power Plant and Simulation of the Radioactive Material Dispersion, Environment. Technology. Resources. Rezekne, Latvia Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 213-217, Environment. Technology. Resources. Rezekne, Latvia Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 213-217, DOI: <https://doi.org/10.17770/etr2025vol5.8468>
- [16] Vambol , S., M. Alqahtani , F., Todorov Dolchinkov , N., Ilyas , M., Yermenko , S., Sydorenko , V. ... Dzhulai , O., (2025), Investigation of the Transfer of Radioactive Contamination from the Chernobyl Zone and its Impact on Radiation in the Environment., Ecological Engineering & Environmental Technology, 25(12), 2024, ISSN 2719-7050, pp . 70-84. <https://doi.org/10.12912/27197050/193261>
- [17] Dolchinkov N., (2025), Management of Plastic Waste Processing and Recycling in Water Pollution Reduction , Economics Ecology Socium , Volume 9, Issue 3, 2025, e-ISSN 2786-8958, ISSN-L 2616-7107, <https://doi.org/10.61954/2616-7107/2025.9.3-5>, pp. 62-78
- [18] Azarov SI (2011), Doslidzhennia approach 137 Cs in the atmosphere from forest fire in Chernobyl zone / SIAzarov , VLSydorenko , OVRudenko , AVPruskiy // Pozhezhna bezpeka : teoriia i praktyka . – 2011, – No. 9. – P. 5–10.
- [19] Suleymanov, A. (2018). Theoretical and tactical bases of providing of safety at emergencies . Lap Lambert Academic Publ .
- [20] Aripkhodzhaeva , MB, Suleimanov , AA (2019). Adaptability of units in complex emergency conditions using UAVs : The article describes the improvement of the adaptability of units in complex emergency conditions using drones (1st edition). Lap Lambert Academic Publishing . <https://nbn-resolving.org/urn:nbn:de:101:1-2019111804353795315711>
- [21] SP Abduraxmonova NG , Xolmatova S. SH. , Nasirova SH. M. , Narziyev EN Yusupxodjayeva (2020), Problems of ensuring the safety of sports activities and reducing injuries , Journal of Critical Reviews , Vol 11, ISSN-2394-5125 Vol 7, pp . 428-432
- [22] Dolchinkov N., Mirsharipova ZM, Aripkhodzhaeva MB (2025), Decision support system for rescuers' safety based on biomonitoring and geographical information system (GIS), "Emergencies And Fire Safety. Problems And Innovations " Scientific And Technical Electronic Journal , ISSN: 3060-5016, 2025 vol 3, pp 12-18
- [23] Agzamova IA, Adilov AA , (2011) Urban Zoning Based on Aggressiveness and Corrosion Properties . Republican Scientific and Technical Conference . Collection of Abstracts . - Tashkent , 2011, pp . 189-191.
- [24] Khasanova OT (2020), Problems of Protecting Aboveground Structures from Aggressive Environments . Problems and Prospects of Innovative Engineering and Technologies in Environmental Protection . International Scientific and Practical Online Conference . September 17-19, 2020. pp . 462-464.
- [25] Khasanova OT, Nizamova DO (2020), Problems of the Environmental Situation in Reservoirs : The Aydar-Arnasai Lake System as an Example . Ecology security current problems . Republic scientific-practical conference materials collection . Uzbekistan Republic national guard military-technical institute . September 15 , 2020 . pp . 99-102
- [26] Gribov VG (2020), Establishment of methods of innovative development in the field of training for law enforcement professionals [Gribov VG, Melnikov VL, Chobitko II // Current problems of ensuring the national security of the state : abstracts of the 3rd International Scientific and Practical Conference (leaf fall 26, 2020). – K.: Institute of Passworld of Ukraine , 2020. pp . 23-25.

- [27] Griban VG (1998), Comparative characteristics of some forms of response construction in programmed learning in human and animal physiology // Proceedings of the Republican scientific-methodological conference him/her issues of scientific organization of the educational process and application of technological methods of teaching . Tbilisi , 28 p.
- [28] Anichkin I.Yu. (2016), Case technology in the distance learning system // Innovative technology in teaching / Proceedings of the 1st international scientific-methodological conference . - Tyumen , 2016, pp . 40-42.
- [29] Karalliedde, L., Wheeler, H., Maclehorse, R., and Murray, V., (2000), Possible immediate and long-term health effects following exposure to chemical warfare agents . Public Health 4(114): 238-248.
- [30] Waysbort, D., Manisterski, E., Leader, H., Manisterski, B., and Ashani, Y., (2004), Laboratory Setup for Long-Term Monitoring of the Volatilization of Hazardous Materials : Preliminary Tests of O-Ethyl S-2-(N,N-Diisopropylamino)ethyl Methylphosphonothiolate on Asphalt. Environmental Science and Technology 7(38): 2217-2223.
- [31] Columbus, I., Waysbort, D., Marcovitch, I., Yehezkel, L., and Mizrahi, DM, (2012), VX fate on common matrices: Evaporation versus degradation. Environmental Science and Technology 7(46): 3921-3927.
- [32] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Improvement of Constructive-Technological Approaches Reducing Innovative Obsolescence of Industrial Technologies in the Context of Industry 4.0, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 180–186.
- [33] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Study of the State of Innovation Development and Obsolescence in the Republic of Bulgaria of Companies from the Mechanical Engineering Sector, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 187–194.
- [34] Petrova, D., Innovative Obsolescence in Mechanical Engineering and Singleness of Indicators, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2024, 3, pp. 221–224.
- [35] Toneva, D., Dimitrova, D., Some aspects of the water crisis in Bulgaria, 5th International Scientific Practical Conference „Environment. Technology. Resources“, Published by Rezekne Academy of Technologies, Latvia. Volume I, pp. 373-377, ISSN 1691-5402, ISBN 978–171389957–0.
- [36] Rachovski, T., Petrova, D., Ivanov, I., Automated Creation of Educational Questions: Analysis of Artificial Intelligence Technologies and Their Role in Education, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2024, 2, pp. 465–467.
- [37] Petrova, D., An Approach to Modeling Innovation Obsolescence, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 175–179.
- [38] Loktionov, O.A., Fedotova, E.V., Kondrateva, O.E., Dolchinkov, N.T., Kuznetsov, N.S. Actual and design wind loads for overhead transmission lines in the Central European part of Russia, IOP Conference Series: Earth and Environmental Science This link is disabled., 2023, 1281(1), 012050
- [39] L. Poiša, L. Antypova, Evaluation of the Effects of Herbicides on the Weeds and the Productivity of Hybrids Maize. Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 14 th International Scientific and Practical Conference, vol. 1, pp. 195–199, Jun. 2023, <https://doi.org/10.17770/etr2023vol1.7204>.
- [40] Stanchev G., Technical obstacles to speech intelligibility, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 3, pp 300-305
- [41] Simeonov M., M. Marinov, Determine the location of nodes in wireless sensor network by using genetic algorithm, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 2, <https://doi.org/10.17770/etr2024vol2.8059> pp 247-252
- [42] N. I. Padarev, Adjusting the Quantity of Surfactants in Decontamination Solutions. Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 219-223, DOI: <https://doi.org/10.17770/etr2025vol5.8469>
- [43] Bulatom. (2022). Nuclear Energy - The Basis for Sustainable Development. <https://www.bulatom-bg.org/> [Accessed: Feb. 13, 2026].
- [44] Council of Ministers of the Republic of Bulgaria. (2020). Integrated Plan in the Field of Energy and Climate of the Republic of Bulgaria 2021 – 2030. Author. [Accessed: Feb. 13, 2026].
- [45] Council of Ministers of the Republic of Bulgaria. (2019). Resolutions and decisions of the Council of Ministers of the Republic of Bulgaria, Sofia. Author. [Accessed: Feb. 13, 2026].
- [46] Dolchinkov, N., & Karaivanova-Dolchinkova, B. (2021). Modern plans for development of production of electricity worldwide and energy independence of Bulgaria, Scientific conference “Radiation safety in the modern world”, NSU “V. Levski”, 392-399.
- [47] Haralampiev, M. (2020). The development of atomic energy and nuclear arsenals. Collection of reports from the Scientific Conference “Current Security Issues”, 6, 123-133.
- [48] IAEA. (2023, May 1). International Atomic Energy Agency. <https://www.iaea.org/> [Accessed: Feb. 13, 2026].
- [49] Dolchinkov N., N. Nichev, Gamma-background radiation control systems as a factor of Bulgaria's national security, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume IV, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2024vol4.8225>, pp 83-88
- [50] Dolchinkov N., Karaivanova-Dolchinkova, B.E., Impact of Types of Electromagnetic Radiation on Living Nature, 14th International Scientific and Practical conference Environment. Technology. Resources. Vide. Technology. Resursi, 2023, ISSN 1691-5402, 1, pp. 55–59

Use of Mobile Autonomous Systems to Control Pollution of Continental Water Bodies

Nikolay Dolchinkov

Vasil Levski National military University, Bulgaria bul.76,

Veliko Tarnovo, 5000, Bulgaria

E-mail: n.dolchinkov@abv.bg,

ORCID: [0000-0002-6171-6083](https://orcid.org/0000-0002-6171-6083)

Abstract — Pollution of continental water resources has emerged as one of the most significant environmental problems in recent decades. This affects both the natural ecosystems inhabiting water areas and the quality of life of the population. The unregulated disposal of large amounts of plastic, construction and household waste into rivers, lakes and adjacent territories leads to significant consequences - degradation of biodiversity, disruption of natural hydrological processes, as well as crises such as floods, pollution of groundwater and drinking water. This study examines the possibilities of applying autonomous technical means - both aerial (drones) and floating (robotic platforms) - for monitoring and control of pollution. These technologies offer a number of advantages: effective monitoring of large areas with minimal resources, the possibility of early detection of unregulated landfills, as well as rapid response to risky situations

Keywords — environment, pollution, aircraft, vessels, control, water surface.

I. INTRODUCTION

The article examines the opportunities and challenges of using mobile autonomous systems for monitoring, early detection and local remediation of pollution in rivers, lakes, water channels and adjacent territories [1, 2]. The main types of autonomous platforms, key sensor and communication solutions, application examples and operational concepts, as well as the legal and institutional context and recommendations for implementation within the framework of integrated water resources management are presented [3, 4, 5].

Inland water bodies are vital for ecosystems, drinking water supplies, agriculture and industry. Traditional methods of pollution control — stationary stations and periodic sampling — often do not provide the spatial and temporal coverage necessary for early detection of incidents and for monitoring dynamic processes such as pollutant dispersion and mass algal blooms. Mobile autonomous systems offer the possibility of flexible,

frequent and targeted monitoring that complements and extends classical approaches [6, 7].

II. MATERIALS AND METHODS

Modern platforms and technologies are used in the monitoring of water bodies and their adjacent territories, with some of the most commonly used being autonomous surface platforms.

Autonomous Surface Vessels (ASVs) are designed for long-duration sampling and measurement missions along defined trajectories, combining GNSS navigation, precision propulsion, and modular sensor architecture (DO, pH, conductivity, chlorophyll, turbidity, etc.). Commercial and research solutions are already demonstrating the great potential for autonomous transects, integration of battery systems, and connectivity to ground stations for real-time data transmission.

In recent years, autonomous underwater vehicles (AUVs) and remotely operated underwater robots (ROVs) have been increasingly used. They allow exploration of the water column and bottom, leak detection, sample collection, and visual inspection using cameras and sonar. These systems are particularly useful for sediment mapping and locating sunken waste or contaminants [8, 9, 10].

For a more complete picture of observations and research, various types of aerial and ground unmanned systems are also used.

Drones (UAVs) provide rapid survey of large areas, detecting oil slicks, floating debris and coastal pollution using multispectral and thermal cameras. Ground-based autonomous platforms and robotic shoreline systems support waste collection and inspection of adjacent areas.

Here we will look at airborne (UAV) and surface water (ASV/USV) pollution monitoring in continental water bodies: what sensors and platforms are used, how data is processed (algorithms and machine learning), operational

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.190>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

workflows, and main limitations when applied in field conditions.

Various platforms and sensors are used for aerial surveillance (UAV), and we will provide a brief overview of the most commonly used ones.

Multispectral cameras (4–8 channels) and RGB cameras for rapid mapping of surface anomalies such as oil slicks, floating debris, and coastal pollution.

Hyperspectral sensors for detection and quantification of chlorophyll a and differentiation of algae species in blooms (HABs) through specific spectral signatures.

Thermal cameras and NIR channels for detecting temperature anomalies and differences in reflectivity between water and oil films [11].

Various algorithms and information processing are used when processing information and analyzing the received data.

Deep neural networks (e.g. U-Net, YOLO variants) are used for segmentation and detection of oil and waste spills on a water surface, and also create models trained on multispectral input data, increasing accuracy in complex conditions (waves, reflections, vegetation).

For HABs, spectral indices and machine learning are used to estimate chlorophyll-a concentrations and distinguish cyanobacteria from other phytoplankton groups [12, 13].

When conducting observations, it is necessary to carry out mission planning and operational practices, such as:

Altitude and overlap: low flights (10–120 m) with high overlap for detailed maps; choice depends on sensor resolution and wind conditions.

Surveillance frequency: regular flights (daily/weekly) in critical areas are recommended for early detection of incidents; in the event of an event, intensive mapping and tracking missions are recommended.

When making observations, it is necessary to take into account some limitations such as cloud cover, strong wind, reflections and shadows, which can reduce the quality, when planning them. When making observations and collecting information, ground validation (samples) is necessary for model calibration [14].

In parallel with aerial monitoring, it is necessary to carry out surface water monitoring (ASV / USV) to obtain more complete and reliable data. It is especially important to select the right platforms on which to deploy the equipment and to take into account the payload of the platform. One of the most widely used are autonomous surface vessels (ASV / USV) with a modular architecture for the integration of various equipment to measure pH, dissolved oxygen (DO), conductivity, turbidity, chlorophyll- fluorimeters, spectrometers and automatic samplers (against contamination).

III. RESULTS AND DISCUSSION

have been built that combine mechanical modules for collecting floating debris or filtering oil slicks, as well as solar charging for extending missions.

According to the sampling and measurement methods used, they can be categorized according to the following indicators:

1. Discrete samples: automatic samplers (syringe - type or piston) allow storage of multiple samples along a trajectory for laboratory analysis; this is important when monitoring toxic substances and microbiological parameters.

2. Continuous sensors: embedded sensors provide time series and allow mapping of spatial variability of parameters in real time.

The autonomous air, ground and water vehicles used must be reliable and provide reliable information. It is of utmost importance that they have a good navigation system and are reliable and safe.

ASVs must integrate GNSS, inertial systems and obstacle avoidance systems (LIDAR/camera/radar) for safe operation in shipping areas, and in limited communication, they execute local plans and buffer data for later transmission.

The use of these means to control pollution of water bodies must be in synergy between air and surface [15].

Tandem and swarm operations are used to fully map the surveyed area.

UAV → ASV workflow, where the drone performs rapid mapping and localizes anomalies, and then the ASV heads to the areas for detailed measurements and sampling. This approach optimizes resources and speeds up incident response.

ASV swarms can cover large areas in parallel, distribute sampling, and maintain continuous monitoring, while UAVs provide an operational picture from above.

Multisensor fusion combines multispectral or hyperspectral imagery with in-situ measurements (pH , DO, chlorophyll) to provide more reliable estimates and calibration of remote sensing; this improves quantitative estimates (e.g. chlorophyll-a concentration) and reduces false alarms.

At the same time, automated workflows are also being applied, such as cloud platforms for ingest, pre-processing (reflection correction, georeferencing), model inference (detection/ classification), and visualization in GIS for rapid decision-making.

In recent years, a lot of practical experience has been accumulated and the following practical considerations and recommendations for more effective activity and more accurate results can be formulated [16].

1. Calibration and validation, which involves regular field calibration of sensors and comparison of remote assessments with laboratory samples, are essential for reliable and accurate results.

2. Communications and processing, creating an architecture with local storage and asynchronous transmission upon connection recovery. In critical incidents, there should be a channel for priority transmission of compressed maps and alarms.

3. Energy and autonomy, which applies the use of energy-efficient missions, solar charging, and trajectory optimization to extend the operating time of ASVs and UAVs.

4. Regulations and safety in compliance with aviation and water regulations, flight zones, permits for operation over populated areas and collision avoidance procedures.

The concept of coordinated teams of heterogeneous autonomous platforms (ASV, AUV, UAV) allows for task separation: rapid mapping from the air, followed by detailed measurement and local cleaning by surface and underwater robots. Swarm approaches improve the coverage and resilience of operations through distributed autonomy and adaptive planning [17].

The use of these monitoring systems has wide application for pollution control.

1. Enable continuous monitoring and early warning. Mobile autonomous systems can perform regular transects and provide real-time data on key water parameters, allowing early detection of deviations from the norm and rapid response to incidents [18]. Integration with cloud platforms and machine learning facilitates automatic classification of events (e.g. blooms, oil spills) and prediction of spread.

2. Localized cleaning and collection of litter, where robotic “cleaning” platforms designed for coastal areas and ports are already being used to collect floating plastic litter and prevent it from entering larger bodies of water. The combination of visual detection and mechanical collectors allows for the creation of “clean corridors” near the shore [19].

3. Coordinated strategies are being developed for oil spills, where swarms of autonomous platforms map the spill, localize the source, and implement local containment and collection measures (floating barriers, filtration modules). Research shows that heterogeneous teams can speed up the response and reduce environmental damage with proper coordination and trajectory modeling.

To implement the activity of controlling the pollution of water bodies, it is necessary to observe a legal framework and integration in water management [32].

The European Water Framework Directive sets targets for achieving “good status” for water bodies and requires monitoring programmes and pollution reduction measures. Autonomous systems can contribute to meeting these requirements through increased spatial and temporal coverage, but their implementation requires data standardisation, sensor certification and clear regulation of operational procedures. Political and institutional barriers are often linked to a lack of funding, insufficient

coordination between agencies and the need to train staff to use the new technologies.

The technical and operational challenges to detecting plastic waste pollution in water bodies are:

1. High quality and calibration of sensors, because mobile platforms use a variety of sensors and maintaining accuracy and calibration in field conditions is critical for reliable data.

2. Energy autonomy, because battery limitations limit the duration of missions, and this can include solutions that include solar charging, hybrid systems, and trajectory optimization.

3. Excellent communications and data transmission, because in remote areas the connection can be unstable. An architecture for local data storage and asynchronous transmission upon connection recovery is required.

4. Good navigation, reliability and safety. Autonomous platforms must avoid collisions with vessels and operate in complex hydrodynamic conditions. This requires reliable localization systems and adaptive planning.

5. Ethics and liability, with clear rules for liability for damage, loss of platforms, or wrongdoing, are needed before widespread deployment.

Swarms of small autonomous platforms can perform parallel tasks (scanning, sampling, waste collection) and reallocate resources in real time based on detected anomalies, which increases the efficiency and resilience of operations [26], [31].

For sustainability, it is important that data and results are accessible to local authorities, water operators and civil society organizations. Training and joint pilot projects facilitate the adoption and proper use of technologies.

Recommendations for implementing these systems can be formulated as follows:

1. Pilot projects in priority basins with clearly defined objectives (monitoring, early warning, cleanup) and evaluation of effectiveness.

2. Data standardization and calibration through certified procedures and compatible exchange formats.

3. Integrated operations centers that coordinate UAV/ASV/AUV missions and provide liaison with rapid response institutions.

4. Financial and regulatory incentives for deployment, including public-private partnerships and innovation programs.

5. Development of swarm and coordination algorithms for optimal use of heterogeneous platforms in incidents such as oil spills [17], [27].

When flying in adverse weather conditions — fog, heavy rain, or snowfall — safety must be the top priority. Flights should be postponed whenever possible if conditions compromise safe operation. Fog greatly reduces

visibility and complicates visual navigation; in such situations, drones equipped with thermal and infrared cameras can assist with orientation and object detection. Heavy rain poses a risk to many drone models because most are not waterproof and can be damaged by moisture ingress. For operations in rain, it is important to use platforms specifically designed to be water-resistant and to apply additional protective measures for the electronics. Snowfall combines reduced visibility with the risk of freezing mechanical and electrical components. Drones with cold-resistant materials and components, together with thermal sensors, can facilitate operations in these conditions, but strict preflight checks and safety procedures remain essential [24], [30], [36], [38].

Practical Measures and Recommendations for Safety

1. Preflight inspections: check seals, battery condition, sensor functionality, and protective coverings.
2. Platform selection: choose drones with appropriate ingress protection and low-temperature ratings for the expected conditions.
3. Sensor suite: combine visual cameras with thermal and infrared sensors for more reliable detection in low-visibility situations.
4. Mission limits: shorten flight durations and avoid risky maneuvers in bad weather; plan contingency options for safe landing.
5. Postflight maintenance: dry and inspect components after exposure to moisture or ice.

During the study it was found that in Bulgaria, besides the Yambol municipality, the Sofia municipality and the Burgas municipality are using marine drones and artificial intelligence to detect potential pollution risks to habitats in the Black Sea. This initiative is part of a project supporting the blue transformation of the Black Sea basin. These are still early tests of drone use in this area, which is typical for the adoption of new technologies — projects usually start with pilot trials and expand gradually [20], [25], [33], [39].

One of the monitoring systems in Europe is the Copernicus Marine Service, which integrates multiple observation sources. European countries use a combination of techniques to monitor plastic waste: numerical modeling, on-site monitoring, and satellite observation. These methods help track the movement of debris, estimate quantities, and plan targeted cleanups. The outlook is to expand monitoring to more water bodies and their surrounding areas, with a significant portion of surveillance carried out by drones [17], [21], [28], [37].

Around the world, different technologies are applied to detect and track plastic waste in the oceans. Ocean current modeling and satellite observation are key methods for following debris distribution and assessing impacts on marine ecosystems. Satellite imagery can reveal large accumulations of plastic in open waters. In coastal zones, especially in tropical regions such as parts of the Pacific with dense vegetation, coastal monitoring drones are particularly important for rapid mapping and pollution assessment [22], [29], [34], [40].

Selected Successful Projects and Examples

- HESOFF (LIFE): uses drones for remote forest imaging and health assessment; it demonstrates how unmanned platforms support biodiversity conservation and forest resource management.
- WWF projects: employ drones to monitor forests and wildlife in various regions; these initiatives show the effectiveness of drones as tools for environmental protection and climate action [17], [23], [34], [41].

IV. CONCLUSIONS

Mobile autonomous systems represent significant potential for improving pollution control in inland water bodies and adjacent territories. They complement traditional methods through greater spatial and temporal coverage, rapid response capabilities, and local cleanup. To realize this potential, coordination between technologies, regulations, and institutions, data standardization, and pilot implementation within existing legal mechanisms for water management are needed.

Combining multispectral/hyperspectral UAV missions with modular ASV platforms and integrated data processing provides a powerful toolkit for early detection, mapping and local response to pollution in inland water bodies. Effective implementation requires rigorous calibration, standardized workflows and coordination between operators, laboratories and regulatory authorities.

The future of drones in environmental protection looks promising, as they are expected to play an increasingly important role in various aspects of environmental monitoring and management. Based on the study conducted, the analysis of the results achieved so far in the use of drones for detecting plastic waste, and the assessment of the future use of these progressive technologies, some conclusions and recommendations can be drawn for the development of the use of these techniques and technologies. Here are some key trends and technologies that will shape the future of drones in this area based on this study:

1. With the development of artificial intelligence and machine learning, drones will become increasingly autonomous, which will allow them to perform complex tasks without the need for constant human control. It will be necessary for a person to set the parameters of the task and control its execution, and the activities themselves will be performed by autonomous drones
2. Drones will be connected and integrated with IoT (Internet of Things), with networks of sensors and other devices, which will allow for the collection and analysis of data in real time for better environmental management. This will allow for larger databases to be collected, which will make research more accurate and forecasts better.
3. The development of new and more sensitive sensors and cameras will allow for more precise detection and monitoring of pollution and other environmental problems. Less time and resources will be needed to assess the situation and make an adequate decision.

4. Drones will increasingly use renewable energy sources, such as stand-alone solar panels, to reduce their carbon footprint and be more environmentally friendly.

As prospects for the use of drones in the foreseeable future, the following can be mentioned:

1. Drones will continue to play a key role in the detection and monitoring of air, water and soil pollution. They will be an indispensable tool for detecting pollution of water bodies and their adjacent territory by plastic waste.

2. They will be used to track wildlife populations and detect illegal activities such as poaching. They will help to expand biodiversity and preserve the purity of the environment.

3. Drones will help to quickly assess damage after natural disasters and plan restoration activities. They will help to locate injured people and rescue them.

These trends and technologies show that drones will continue to be an important tool in efforts to protect the environment and sustainably manage natural resources.

In Bulgaria, work is underway to increase the use of drones in state, municipal and private structures, and they are also used in a number of projects, and emphasis will be placed on several of them:

A project for the blue transformation of the Black Sea basin has the Municipality of Burgas as the main beneficiary. Municipal administration employees are using marine drones and artificial intelligence to detect potential risks of pollution of habitats in the Black Sea. This project is part of a larger initiative to protect the marine environment and is about to be expanded.

The HESOFF project, which is funded under the LIFE program and monitors the environment, including water bodies. This project involves remote sensing of forests with unmanned aerial vehicles to assess the health of forests, the state of water bodies in them and the protection of biodiversity.

These projects show how Bulgaria strives for sustainable development and environmental protection through innovation and new technologies, including the use of unmanned aerial vehicles. Based on the research conducted, the analysis of the results obtained and the identified prospects for the use of drones in environmental monitoring, and in particular of water bodies and adjacent terrains, we can summarize that a wider use of drones in environmental protection is imminent.

REFERENCES

- [1] Vassilev G., Radioecology, Tita Consult, Sofia, 2005
- [2] Dolchinkov N., Karaivanova-Dolchinkova, BE, Impact of Types of Electromagnetic Radiation on Living Nature, 14th International Scientific and Practical conference Environment. Technology. Resources. Vide. Technology. Resources, 2023, ISSN 1691-5402, 1, pp. 55–59
- [3] S. Madzharov, I. Ivanov, N. Yordanov, A Digitally Manipulated Gunshot Sound Identification. In Environment. Technologies. Resources. Proceedings of the International Scientific and Practical Conference, 2024, Vol. 3, pp. 170-174, ISSN: 16915402, <https://doi.org/10.17770/etr2024vol3.8150E>.
- [4] T. Trifonov, I. Simeonov, N. Yordanov, Advanced signal processing methods for analysis of high dynamic range acoustic phenomena, Communication, Electromagnetics and Medical Application, 2018, October, pp. 52–56.
- [5] M. Musaevev, A. Boboev, and E. Arziyev, Formalization of tasks to ensure the safety of emergency and explosive operations in the mining industry, ETR, vol. 1, pp. 257–260, Jun. 2024, <https://doi.org/10.17770/etr2024vol1.8007>
- [6] Tsvetkov R. Electromagnetic fields created from mobile devices and methods for hygienic protection, Collection reports from International scientific conference "Radiation" safety in modern times world", volume 2, National University "Vasil Levski", Veliko Tarnovo, 2025, ISSN 2738-7607, pp. 150-155, <https://doi.org/10.34660/INF.2025.23.39.048>.
- [7] Simeonov M., M. Marinov, Determine the location of nodes in wireless sensor network by using genetic algorithm, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 2, <https://doi.org/10.17770/etr2024vol2.8059> pp 247-252
- [8] Koynakov K., Research of the energy status of military personnel during complex tactical exercises, Environment. Technology. Resources. Rezekne, Latvia Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 135-139
- [9] Nichev N., Koynakov K., A model for using drones for medical reconnaissance in combat operations, Environment. Technology. Resources. Rezekne, Latvia Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 209-212
- [10] Nedev, N., Specificity on the international humanitarian right in the conditions on modern armed conflicts, Scientific Conference "Knowledge, Science, Innovations, Technologies", December 13, 2024, Veliko Tarnovo, ISSN 2815-3480 (CD), pp. 1455-1468.
- [11] Dolchinkov N., Optimizing energy efficiency in the conditions of a global energy crisis, Optimizing Energy Efficiency During a Global Energy Crisis, 2023, ISBN13: 9798369304006 EISBN13: 9798369304013, <https://doi.org/10.4018/979-8-3693-0400-6> pp. 1–9
- [12] Dolchinkov N., Ozerova NV, State of recycling of waste in Bulgaria, International scientific journal: Science. Business. Society 4/2019, ISSN 2367-8380 pp. 131-134;
- [13] Tsvetkov. R. Risks of increasing the specific absorbed power (SAR) when using mobile devices. Proceedings of the International Scientific Conference "Radiation Safety in the Modern World", volume 3, National University "Vasil Levski", Veliko Tarnovo, 2025, ISSN 2738-7607, pp. 67-72, <https://doi.org/10.34660/INF.2025.47.94.066>.
- [14] Milen Simeonov, Penyo Penev, NASA's scientific research campaigns - benefits and prospects for development, Collection of reports from the scientific conference "Near Space - a common goal", May 10-11, 2022, Publishing Complex of the National University of Science and Technology "Vasil Levski", ISSN 2815-3510 Print, ISSN 2815-3529 CD
- [15] Dimitar Dimitrov, Evgeni Andreev, Development of computer simulations of objects on the lunar surface under the international simulation program exploration experience, Collection of papers from the scientific conference "Near Space - a common goal", May 10-11, 2022, Publishing Complex of the National University "Vasil Levski", ISSN 2815-3510 Print, ISSN 2815-3529 CD
- [16] Dolchinkov N., Sergey Vambol, Viola Vambol, Barbara Savitska, Measures to reduce plastic waste in water bodies, Scientific Conference "Radiation Safety in the Modern World", National University "V. Levski" - city of Veliko Tarnovo - March 18-20, 2025, ISSN 2738-7607 Print, ISSN 2603-4689 CD, <https://doi.org/10.34660/INF.2025.97.57.056>, volume 2 pp. 217-231

- [17] Dolchinkov N., N. Nichev, Using Drones to Clean Continental Water Bodies, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 16th International Scientific and Practical Conference. 2025 Volume V, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2025vol5.8501.89-96>
- [18] Dolchinkov N., Building a System for Monitoring and Controlling Pollution of Water Bodies, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume I, Print ISSN 1691-5402, Online ISSN 2256-070X, https://dx.doi.org/10.17770/etr2025volI.8693_village.171-177
- [19] Dolchinkov N., Management of Plastic Waste Processing and Recycling in Water Pollution Reduction, Economics Ecology Socium, Volume 9, Issue 3, 2025, e-ISSN 2786-8958, ISSN-L 2616-7107, <https://doi.org/10.61954/2616-7107/2025.9.3-5>, pp. 62-78
- [20] Stefanova, D.P., Vasilev, V.P., Efremovski, I.P. (2023). Re-innovative organizational design: sustainable branding and effective communication - applied models in a world with new borders/without borders, Book Chapter: Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing, pp. 112–127; <https://doi.org/10.4018/978-1-6684-8681-8.ch006>
- [21] Dolchinkov N., . Construction Of A System For Monitoring The Pollution Of Water Bodies With Waste, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume I, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2024volI.7989>, pp 136-141
- [22] Dolchinkov N., Karaivanova-Dolchinkova, B.E., Impact of Types of Electromagnetic Radiation on Living Nature, 14th International Scientific and Practical conference Environment. Technology. Resources. Vide. Technology. Resursi, 2023, ISSN 1691-5402, 1, pp. 55–59
- [23] Haralampiev M., Global environmental problems and their relationship with the protection of the population and infrastructure, Collection of reports from the scientific conference "Actual problems of the protection of the population and infrastructure", Vasil Levski, Veliko Tarnovo, 2012, volume 4, pp. 34-49, ISBN 978-954-753-104-8;
- [24] Dolchinkov N., . Construction Of A System For Monitoring The Pollution Of Water Bodies With Waste, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume I, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2024volI.7989>, pp 136-141
- [25] Petrova, D., An Approach to Modeling Innovation Obsolescence, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 175–179.
- [26] Vassilev G., Radio ecology, Tita consult, Sofia, 2005;
- [27] Vasilev, V., Stefanova, D., Popescu, C. (2023). Human capital management and digitalization - From good practices and traditions to sustainable development; Book Chapter: Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, pp. 41–65; <https://doi.org/10.1108/978-1-83753-190-520231004>
- [28] Dimitrov B., Problems in the special preparation for nuclear, chemical and biological protection, Collection of reports from a scientific conference, IV International Scientific Conference High Technologies. Business. Society 11-14.03.2019, Borovets, Bulgaria, Volume Iii "Society", pp. 263-265, ISSN 2535-0005
- [29] Loktionov, O.A., Fedotova, E.V., Kondrateva, O.E., Dolchinkov, N.T., Kuznetsov, N.S. Actual and design wind loads for overhead transmission lines in the Central European part of Russia, IOP Conference Series: Earth and Environmental Science This link is disabled., 2023, 1281(1), 012050
- [30] L. Poiša, L. Antypova, Evaluation of the Effects of Herbicides on the Weeds and the Productivity of Hybrids Maize. Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 14 th International Scientific and Practical Conference, vol. 1, pp. 195–199, Jun. 2023, <https://doi.org/10.17770/etr2023vol1.7204>.
- [31] Stanchev G., Technical obstacles to speech intelligibility, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 3, pp 300-305
- [32] Simeonov M., M. Marinov, Determine the location of nodes in wireless sensor network by using genetic algorithm, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 2, https://doi.org/10.17770/etr2024vol2.8059_pp.247-252
- [33] V. Vasilev, D. Stefanova, and M. Icheva (2024). Green human resource management as a component of sustainable organizational development in environmental and natural economics, ETR, vol. 1, pp. 402–407, Jun. 2024, <https://doi.org/10.17770/etr2024vol1.7966>
- [34] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Improvement of Constructive-Technological Approaches Reducing Innovative Obsolescence of Industrial Technologies in the Context of Industry 4.0, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 180–186.
- [35] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Study of the State of Innovation Development and Obsolescence in the Republic of Bulgaria of Companies from the Mechanical Engineering Sector, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 187–194.
- [36] Petrova, D., Innovative Obsolescence in Mechanical Engineering and Singleness of Indicators, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2024, 3, pp. 221–224.
- [37] Toneva, D., Dimitrova, D., Some aspects of the water crisis in Bulgaria, 5th International Scientific Practical Conference „Environment. Technology. Resources“, Published by Rezekne Academy of Technologies, Latvia. Volume I, pp. 373-377, ISSN 1691-5402, ISBN 978–171389957–0.
- [38] Rachovski, T., Petrova, D., Ivanov, I., Automated Creation of Educational Questions: Analysis of Artificial Intelligence Technologies and Their Role in Education, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2024, 2, pp. 465–467.
- [39] Aripadzhazeva M.B., Mirsharipova Z.M. Algorithm and mathematical apparatus for determining the critical state of rescuers in extreme situations using innovative technologies // INNOVATION TECHNOLOGIES. — 2025. — No. 1/17. — P. 231-236 . URL: — mvahi.uz
- [40] Suleymanov A.A. , Hasanov O.L. Mechanism of security of security // Actual problems of security of security in Russian Federation.
- [41] Suleymanov A.A. , Hasanov O. About the science that studies development methodologies of the security of security // Actual problems of security of the security in Russian FederationA. Rezi and M. Allam, "Techniques in array processing by means of transformations," in Control and Dynamic Systems, Vol. 69, Multidimensional Systems, C. T. Leondes, Ed. San Diego: Academic Press, 1995, pp. 133-180.
- [42] Georgiev G., People as a resource in the organization, Plovdiv: Academic Publishing House Talent of the Higher School of Agribusiness and Regional Development, 2022. 232 p. ISBN 978-619-203-326-2 (CD)
- [43] Ilcheva M., G. Georgiev, Information and social security – contemporary risks and challenges, KNOWLEDGE, science, innovations, technologies: collection of reports from a scientific conference, Publishing House "Institute for Knowledge, Science and Innovations", Veliko Tarnovo, 1/2024, pp. 1116-1128, ISSN 2815-3480 (CD) [NRS]

Organizing and Conducting Underwater Search and Rescue Operations for Victims

Nikolay Dolchinkov
Vasil Levski National military
University, Bulgaria bul.76,
Veliko Tarnovo, 5000, Bulgaria
E-mail: n.dolchinkov@abv.bg,
ORCID: [0000-0002-6171-6083](https://orcid.org/0000-0002-6171-6083)

Zilola Mirziyatovna Mirsharipova
Tashkent State Technical University,
Uzbekistan, Tashkent
E-mail:
zilola.mirsharipova.71@mail.ru

**Malikahon Bakhtiyarovna
Ariphadzhaeva**
Tashkent State Technical University,
Uzbekistan, Tashkent
E-mail:
zilola.mirsharipova.71@mail.ru

Abstract — A review of modern methods for organizing and conducting rescue operations in water bodies is made. The methods are improved using artificial intelligence (AI) to support rescue divers in underwater operations for searching and rescuing victims in accidents. Modern technologies for processing data obtained from sonar systems, video streams and sensor information are considered. Machine learning algorithms are also presented to improve the accuracy of detecting underwater objects in order to reduce the time required for detecting and extracting victims. It has been proven that the use of AI improves the efficiency of operations, reduces risks to the life and health of divers and shortens the search time.

Keywords — artificial intelligence, rescue divers, underwater search and rescue operations, machine learning, sonar.

I. INTRODUCTION

Search and detection of underwater objects remains one of the most difficult tasks in hydrography, underwater archaeology, maritime safety and rescue operations. Traditional methods of underwater search include visual inspection by divers, the use of sonar and echolocation systems, as well as underwater remotely operated vehicles (ROV) [1, 2]. These methods make it possible to effectively detect objects at shallow depths and in relatively clear water, however, their effectiveness decreases sharply in conditions of poor visibility, strong currents or at great depths [17], [25], [34], [41].

In recent years, the application of artificial intelligence (AI) methods for automating the search and classification of underwater objects has been actively developed [18], [27], [32], [39], [44]. The use of deep learning, ultra-precise neural networks and transformers allows to increase the accuracy of detection, as well as to reduce the time required

for the analysis of large arrays of underwater images and sonar data [3–5], [22], [38].

Modern AI algorithms are integrated with underwater visualization systems, allowing not only to detect objects, but also to classify them by type, size and condition [16], [20], [26], [33]. This is especially important for the tasks of underwater archeology and rescue operations, where reaction time is critical [24], [29], [36], [40], [45].

- Traditional search methods: in the studies of Okorokova [1] and Tufanova [2], algorithms and strategies of traditional search using groups of autonomous underwater devices are described in detail. These methods are well suited for the planned survey of large water areas, but have time and visibility limitations.

- Application of AI in underwater search: Abramov and Petrov [3] proposed algorithms for classification of objects in underwater images using super-accurate neural networks. Abu and Diamant [4] integrated synthetic aperture sonar data and optical images to improve object detection accuracy.

- Integration of AI and autonomous systems: Shishkin and Grekov [5] developed an intellectual system of automatic monitoring of the water environment using compact autonomous robots. Similar systems allow you to quickly receive data and automatically estimate the state of objects [21], [30], [42].

- Overview of theoretical foundations: Shen [6] considers the interdisciplinary application of deep learning in hydrosciences, including tasks of classification and detection of underwater objects. Bongard [7] and Craven [8] describe classical approaches to image recognition and Bayesian search theory, which underlie modern AI algorithms for underwater search [13], [19], [35].

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.191>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Thus, the relevance of research is determined by the need to increase the efficiency of underwater search due to the integration of traditional methods and modern algorithms of artificial intelligence. In modern conditions, the use of AI allows to significantly reduce search time, increase the accuracy of object detection and reduce risks for divers and rescuers [2], [23], [31].

Underwater search and rescue operations (SAR) are one of the most difficult and dangerous types of rescuers' activities. Limited visibility, strong currents, cold water, complex underwater structures and unpredictable weather conditions pose high risks to the life and health of rescue divers. Even experienced specialists face difficulties in orientation under water, detection of objects and assessment of the situation, which can lead to increased search time and increased danger during operations.

An overview of existing research shows that the use of AI allows to significantly improve orientation under water, speed up the search for objects and reduce risks for personnel. The development of machine learning algorithms, computer vision methods and intellectual data analysis systems makes it possible to implement automated diver support tools in real time. In addition, AI-technologies contribute to the reduction of response time in emergency situations and increase the overall efficiency of search and rescue operations [28], [37], [43].

The relevance of the topic is due to the increase in the number of diving operations in complex and extreme conditions, such as heated buildings, marine accidents, river and sea disasters, as well as the growth of requirements for personnel safety. The implementation of AI in underwater search and rescue operations is considered a promising direction that can significantly increase the level of training of rescue divers and the efficiency of rescue operations, as well as reduce risks to the life and health of specialists [4], [45].

II. RESEARCH METHODS

Modern methods of scientific analysis and systematization of information were used to prepare this review. The main stages of the study were:

Search and selection of sources. Publications devoted to the application of artificial intelligence in underwater search and rescue operations were studied, including scientific articles, conference proceedings, technical reports and patents. The main attention was paid to the research of the last five years, which allowed to cover the current achievements in the fields of AI and robotic underwater systems.

Critical analysis of literature. Made an analysis of publications from the point of view of applied technologies, data processing algorithms, computer vision methods, integration with autonomous underwater devices and research results. Special attention was paid to the comparative evaluation of the effectiveness of traditional search methods and methods using AI.

Systematization of information. The collected information was structured in key directions: processing of sonar data, analysis of video streams, prediction of object

movements, decision support and integration with autonomous systems. Such an approach made it possible to identify general trends, advantages and limitations of the use of AI in underwater search and rescue operations.

Synthesis and summary of data. Based on the analysis and systematization of the literature, conclusions were drawn about the prospects of AI application, existing problems and directions of further research in the field of underwater search and rescue.

The use of the specified methods made it possible to prepare a complex overview of existing technologies, assess their practical significance and determine directions for future research.

Advantages and limitations of using AI in underwater search and rescue operations

Application of artificial intelligence in underwater search and rescue operations provides a number of advantages:

1. Increased accuracies of requested objects. AI allows analyzing large arrays of data with sonar and video cameras, identifying objects that are difficult to notice visually, and reducing the amount of false positives [9].

2. Reduction of the time of search operations. Algorithms for predicting the movement of objects and support for decision-making help divers choose optimal routes and quickly reach their goals [10].

3. Risk reduction for divers. The use of intelligent systems makes it possible to limit the stay of divers in dangerous areas, warn about potential threats and increase safety [11].

4. Integration with autonomous systems. A combination of AI with autonomous underwater devices expands the survey area and allows you to perform several tasks at the same time, which increases the efficiency of operations [12].

For a visual presentation of the main technologies of artificial intelligence used in underwater search and rescue operations, table 1 was compiled. It systematizes the key areas of AI application, their functions, main advantages and existing limitations, as well as links to scientific studies confirming the effectiveness of these technologies. The table allows you to visually compare various approaches and understand which methods are most promising for practical implementation.

TABLE 1 BASIC AI TECHNOLOGIES IN UNDERWATER SEARCH AND RESCUE OPERATIONS

AI technology	Functions	Advantages	Restrictions
Processing of sonar data	Analysis of sonar and multibeam sonar signals	Increase in object detection accuracy, decrease in false positives	Dependence on data quality and visibility

Video streaming analysis	Computer vision for object identification and state estimation	Real time analysis, help diver in orienteering	Muddy water, bad sanctification
Forecasting object movements	Modeling of trajectories taking into account currents	Optimization of route requests, shortening of operation times	Algorithmic limitations in complex hydrodynamic s
Decision support	Recommendations on the route, movement speeds and zones requested	Reduction of errors and risk, acceleration of decision-making	Interpretation by specialists is required
Integration with autonomous underwater devices	Joint work of the human and the robot, expansion of the inspection zone	Increase coverage, automate repetitive tasks	High cost of equipment, staff training

Comparison of underwater object search efficiency: percentage of detected objects in time using traditional and artificial intelligence (AI) methods. The curve shows that the application of AI significantly speeds up the search and increases the proportion of detected objects compared to traditional approaches. Fig. 1.

However, there are also limitations:

1. Dependence on data qualities. The effectiveness of AI directly depends on the accuracy and completeness of sonar, sensor and video camera data. In the conditions of muddy water, strong currents or technical problems, the efficiency of algorithms can decrease [13].

2. Complexity of implementations. AI-system integration in underwater operations requires expensive equipment, trained personnel and software adaptations under specific conditions [14].

3. Limited capabilities of autonomous analysis. Despite high computing power, modern AI algorithms are not always able to take into account all factors influencing the complex dynamics of the underwater environment and require the participation of specialists for the interpretation of results [15].

Thus, the use of AI in underwater search and rescue operations is a promising direction, but it requires taking into account limitations related to data quality, complexity of implementation and the need to combine it with human control.

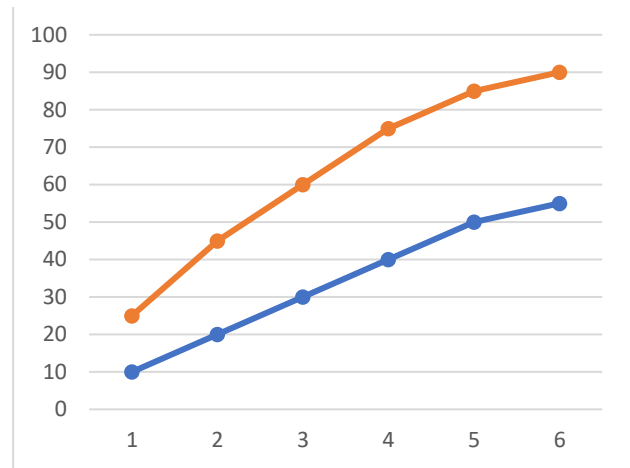


Fig. 1. Underwater object search efficiency: AI (blue) vs. traditional (orange) methods

For papers with fewer than six authors: To change the default, adjust the template as follows.

This section presents the results of the survey conducted among rescuers, indicating the distribution of responses to each question.

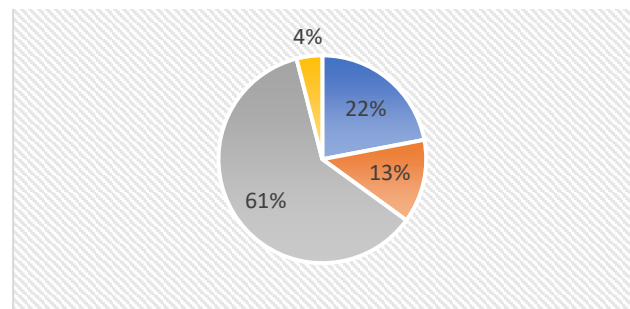


Fig. 2. Distribution of respondents' answers to the question: "Have you used health monitoring devices while at work?"

The majority of respondents (61%) have never used health monitoring devices in the workplace. Only about 22% use them regularly and 13% use them occasionally.

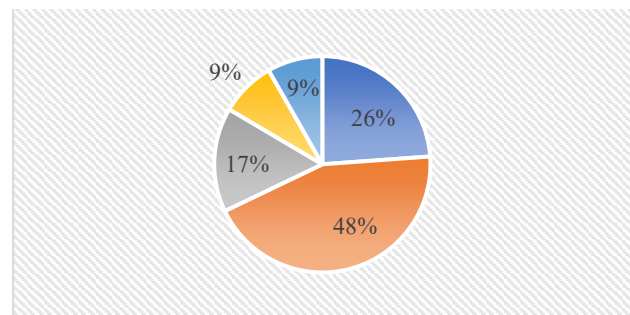


Fig. 3. Distribution of respondents' answers to the question: "What devices have you used or are you familiar with?"

Some respondents indicated multiple devices at the same time.

- The most well-known and used are fitness bracelets/smartwatches – almost half of the respondents.

- About a quarter of those surveyed did not use any devices.
- Heart rate monitors and GPS devices are less common.

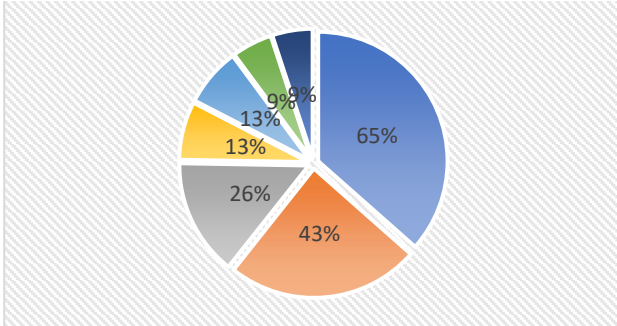


Fig. 4. Distribution of respondents' answers to the question: "Which indicators do you consider important for monitoring the health of a rescuer in real time?"

Most respondents considered comprehensive monitoring (all indicators) important, particularly highlighting the importance of pulse rate and blood oxygen content as key parameters.

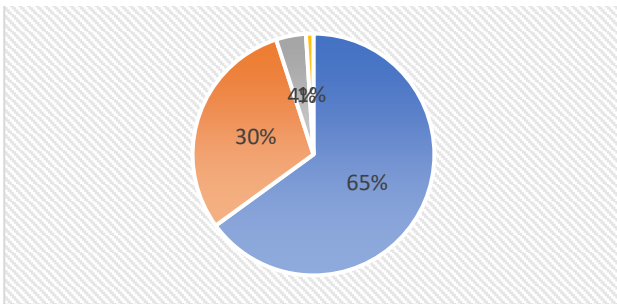


Fig. 5. Distribution of respondents' answers to the question: "Is a health monitoring system necessary at work?"

The majority of respondents (about 65%) positively assess the need for a health monitoring system, with the majority in favor of the mandatory presence of such a system, and some in favor of its convenience and reliability.

Comparison with other studies

Review of similar studies. Research in the field of monitoring the physiological state of rescuers and other emergency care professionals has been actively developing over the past two decades. The most researched areas are real-time monitoring of heart rate, body temperature, blood oxygen saturation and respiratory parameters. A number of international projects (e.g. Dräger systems) Bodyguard, Physiological Condition Monitoring System (developed in the USA for the military) use wearable sensors integrated with a data transmission system to a control panel. Although these solutions have proven their effectiveness in training and real-life situations, their capabilities are limited: in most cases they record only basic parameters (heart rate, temperature, respiration) and do not provide a comprehensive analysis of the rescuer's condition.

Comparison with literature results. Comparison of the data obtained during the study and field trials with relevant publications shows that the established trends are consistent with international experience. For example, studies conducted in Germany and Canada show high interest among rescuers in monitoring technologies, but at the same time document skepticism about their reliability and ease of use in extreme conditions. Our respondents demonstrate similar expectations and concerns: a positive perception of the innovation is combined with doubts about the reliability of the devices. Field trials also confirm the findings of international authors that the accuracy of photoplethysmographic sensors decreases with active movement, and data transmission is complicated by smoke or signal obstructions.

Justification of similarities and discrepancies. The similarity between our data and international studies is evident in the confirmation of the main hypothesis that real-time physiological monitoring is an effective tool for improving personnel safety. The list of key issues is also consistent: sensor reliability, battery autonomy, and communication channel integrity. Our study differs in the extended functionality of the developed system: the inclusion of additional sensors (EEG, non-invasive blood pressure measurement and aspiration flow sensor) allows for a more complete picture of the state of the body and the environment. Moreover, unlike many international developments, which are primarily aimed at military units, our solution is adapted to the specific needs of civil emergency services. This expands the scope of application of the system and increases its importance for ensuring safety in various emergency situations.

III. CONCLUSIONS

An overview of modern research shows that the use of artificial intelligence in underwater search and rescue operations significantly increases the efficiency and safety of the actions of rescue divers. The use of AI allows analyzing sonar data, video streams and sensor information in real time, predicting the movement of objects, supporting decision-making and integrating the actions of divers with autonomous underwater devices.

The main advantages of using AI are: increasing the accuracy of searching for objects, reducing the time of operations, reducing risks for divers and expanding the survey zone with the help of autonomous systems. However, it is necessary to take into account limitations: dependence on data quality, complexity of implementation and the need for a combined approach with the participation of specialists.

Prospective areas of further research include:

Development of more accurate algorithmic data analysis in conditions of limited visibility and complex hydrodynamics.

Integration of AI with new types of autonomous underwater apparatuses for expansion of demand and monitoring.

Creation of hybrid systems combining automated analysis and expert assessment of divers to increase the reliability of solutions.

Thus, artificial intelligence is considered a key tool for modernizing underwater search and rescue operations and improving personnel safety. Further development of technologies and their integration into the practice of diving activities will significantly increase the efficiency of rescue operations and reduce risks to the life and health of specialists.

Practical significance of the obtained data

Relevance and necessity of the implementation of the system. The results of the study show that the implementation of a comprehensive system for physiological monitoring of rescuers is not just a promising area, but an objective necessity. Analysis of a survey revealed that the majority of specialists report high physical and psycho-emotional stress during emergency situations, accompanied by the risk of sudden deterioration of health. However, existing monitoring tools (radio communication, visual observation, periodic reports) do not allow for rapid recording of changes in vital signs. The developed device fills this gap by providing continuous monitoring of body and environmental parameters, increasing the reliability of rescue team operations and reducing the likelihood of critical incidents.

Impact on improving safety and efficiency. During field tests, the system demonstrated its ability to timely record changes in physiological parameters, which allows the operator to remotely detect signs of overload or deterioration of the rescuer's condition. This capability is a key factor in improving safety: when critical values are detected, the operator can decide to evacuate or provide assistance before serious consequences develop. In addition, the presence of a suction flow sensor allows for the assessment of changes in the direction and intensity of air masses, which is especially important when extinguishing fires and responding to accidents involving toxic gases. Thus, the device performs a dual function – monitoring the human condition and monitoring the environment, improving the overall efficiency of rescue services. Prospects for further use and development. The data obtained demonstrate significant potential for further improvement of the equipment. First, the system can be scaled by connecting additional sensors (for example, to measure carbon monoxide levels or background radiation), expanding the range of monitored factors. Second, the integration of intelligent data analysis algorithms will allow not only to record current conditions, but also to predict the development of dangerous situations based on identified patterns. Third, the results can be used in the development of specialized monitoring systems for different categories of workers: firefighters, miners, military personnel, and employees of chemical and oil and gas plants. Thus, the created system is a universal platform capable of further adaptation and implementation in a wide range of professional fields.

REFERENCES

- [1] Okorokov A. V. History of underwater archeology in Russia and the USSR (part 1) // CyberLeninka . – Access mode: <https://cyberleninka.ru/article/n/istoriya-podvodnoy-arheologii-v-rossii-i-sssr-chast-1>.
- [2] Tufanov I. E. Methods of solving survey-search tasks using groups of autonomous uninhabited underwater devices: dis Ph.D. technical Nauk / I. E. Tufanov. – Vladivostok, 2019. – Access mode: https://iacp.dvo.ru/resources/fileman/Uploads/d_tufanov.pdf.
- [3] Abramov I.V., Petrov S.A. Application of artificial intelligence methods for classification of objects in underwater images // arXiv , 2018. – Access mode: <https://arxiv.org/abs/1805.10106>.
- [4] Abu A ., Diamond R. Underwater object classification combining SAS and transferred optical-to-SAS Imagery // arXiv , 2023. – Mode access : <https://arxiv.org/abs/2304.11875>.
- [5] Shishkin Yu . E. , Grekov A. N. Automated Environmental Monitoring Intelligent System Based on Compact Autonomous Robots for The Sevastopol Bay // arXiv , 2021. – Mode access : <https://arxiv.org/abs/2108.11166>.
- [6] Shen Ch . A trans-disciplinary review of deep learning research for water resources scientists // arXiv , 2017. – Mode access : <https://arxiv.org/abs/1712.02162>.
- [7] Bongard M. M. The problem of knowledge. - M.: Nauka, 1979.
- [8] Craven J. P. The Silent War: The Cold War Battle Beneath the Sea. – London: Weidenfeld & Nicolson, 2004.
- [9] Balzannikov M. I. Technical means and methods of effective use of the GAES- VES system: autoref. dis Dr. Tech. Science / M. I. Balzannikov . - M., 2015. - Access mode: https://ru.wikipedia.org/wiki/Balzannikov,_Mikhail_Ivanovich.
- [10] Berezin A. A. Peculiarities of periodization in modern domestic historiography of underwater archeology // CyberLeninka . – Mode of access: <https://cyberleninka.ru/article/n/osobennosti-periodizatsii-v-sovremennoy-otechestvennoy-istoriografii-podvodnoy-arheologii>.
- [11] Chepalyga A. L. World Flood as a real paleohydrological event // Wikipedia. – Access mode: https://ru.wikipedia.org/wiki/Chepalyga,_Andrei_Leonidovich.
- [12] Ereshko F. I. Managing the competitiveness of organizations in the context of import substitution policies. - Moscow: Infra-M, 2018.
- [13] Aripadzhayeva M.B. , Mirsharipova Z.M. Algorithm and mathematical apparatus for determining the critical state of rescuers in extreme situations using innovative technologies // INNOVATION TECHNOLOGIES. — 2025. — No. 1/17. — P. 231-236 . URL: — mvahi.uz
- [14] Suleymanov A.A. , Hasanov O.L. Mechanism of security of security // Actual problems of security of security in Russian Federation.
- [15] Suleymanov A.A. , Hasanov O. About the science that studies development methodologies of the security of security // Actual problems of security of the security in Russian Federation A. Rezi and M. Allam, "Techniques in array processing by means of transformations, " in Control and Dynamic Systems, Vol. 69, Multidimensional Systems, C. T. Leondes, Ed. San Diego: Academic Press, 1995, pp. 133-180.
- [16] Hegarty-Craver, M., Davis-Wilson, H., Gaur, P., Walls, H., Dausch, D., & Temple, D. (2024). Wearable sensors for military personnel and first responders: Considerations for using commercially available sensors for continuous monitoring. RTI Press. <https://doi.org/10.3768/rtipress.2024.op.0090.2402>
- [17] Poh, M. Z., Swenson, N. C., & Picard, R. W. (2010). A wearable sensor for discrete, long-term assessment of electrodermal activity. IEEE Transactions on Biomedical Engineering, 57 (5), 1243–1252. <https://doi.org/10.1109/TBME.2009.2038487>
- [18] Johnstone, J. A., Ford, P. A., Hughes, G., Watson, T., & Garrett, A. T. (2012). BioHarness™ multivariate monitoring device: Part I: Validity. Journal of Sports Science & Medicine, 11 (3), 400–408.

- [19] Khurshid, S., Friedman, S., Reader, K., Di Achille, P., Diamant, N., Singh, P., ... & Lubitz, S. A. (2021). Design and analysis of a wearable cardiac monitoring device. *NPJ Digital Medicine*, 4 (1), 1–10. <https://doi.org/10.1038/s41746-021-00444-6>
- [20] Benedetto, S., Caldato, K., Bazan, E., Greenwood, D. C., Pensabene, V., & Aktis, P. (2020). Evaluation of the Empatica E4 wristband for continuous monitoring of physiological signals in everyday life. *Sensors*, 20 (3), 718. <https://doi.org/10.3390/s20030718>
- [21] Shcherbina, A., Matson, K. M., Wagot, D., Salisbury, H., Crystal, J. W., Hastie, T., & Wheeler, M. T. (2017). Accuracy of wrist-worn heart rate and energy expenditure measurements with sensors in a diverse cohort. *Journal of Personalized Medicine*, 7 (2), 3. <https://doi.org/10.3390/jpm7020003>
- [22] Hagi, M., Turow, K., & Stoll, R. (2017). Wearables in the Medical Internet of Things: Research and Commercially Available Devices. *Healthcare. Informatics Research*, 23 (1), 4–15. <https://doi.org/10.4258/hir.2017.23.1.4>
- [23] Dräger. (2025). MartPASS Advanced Personal Monitoring System. Retrieved August 10, 2025 from https://www.draeger.com/en_uk/Products/MartPASS-Advanced-Personal-Monitoring-System [Accessed: Feb. 23, 2026].
- [24] PyroGuardian. (2025). Firefighter Monitoring System. Retrieved August 10, 2025 from <https://pyroguardian.com/products/> [Accessed: Feb. 23, 2026].
- [25] Dräger. (2025). Bodyguard 1500: Personal Monitoring System. Retrieved August 10, 2025 from <https://www.draeger.com/Content/Documents/Products/bodyguard-1500-pi-9041743-ru-ru.pdf> [Accessed: Feb. 23, 2026].
- [26] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Improvement of Constructive-Technological Approaches Reducing Innovative Obsolescence of Industrial Technologies in the Context of Industry 4.0, *Vide Tehnologija Resursi Environment Technology Resources*Open source preview, 2023, 1, pp. 180–186.
- [27] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Study of the State of Innovation Development and Obsolescence in the Republic of Bulgaria of Companies from the Mechanical Engineering Sector, *Vide Tehnologija Resursi Environment Technology Resources*Open source preview, 2023, 1, pp. 187–194.
- [28] Petrova, D., Innovative Obsolescence in Mechanical Engineering and Singleness of Indicators, *Vide Tehnologija Resursi Environment Technology Resources*Open source preview, 2024, 3, pp. 221–224.
- [29] Toneva, D., Dimitrova, D., Some aspects of the water crisis in Bulgaria, 5th International Scientific Practical Conference „Environment. Technology. Resources“, Published by Rezekne Academy of Technologies, Latvia. Volume I, pp. 373-377, ISSN 1691-5402, ISBN 978–171389957–0.
- [30] Rachovski, T., Petrova, D., Ivanov, I., Automated Creation of Educational Questions: Analysis of Artificial Intelligence Technologies and Their Role in Education, *Vide Tehnologija Resursi Environment Technology Resources*Open source preview, 2024, 2, pp. 465–467.
- [31] Petrova, D., An Approach to Modeling Innovation Obsolescence, *Vide Tehnologija Resursi Environment Technology Resources*Open source preview, 2023, 1, pp. 175–179.
- [32] Vassilev G., Radio ecology, Tita consult, Sofia, 2005;
- [33] Vasilev, V., Stefanova, D., Popescu, C. (2023). Human capital management and digitalization - From good practices and traditions to sustainable development; Book Chapter: Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, pp. 41–65; <https://doi.org/10.1108/978-1-83753-190-520231004>
- [34] Dimitrov B., Problems in the special preparation for nuclear, chemical and biological protection, Collection of reports from a scientific conference, IV International Scientific Conference High Technologies. Business. Society 11-14.03.2019, Borovets, Bulgaria, Volume Iii "Society", pp. 263-265, ISSN 2535-0005
- [35] Loktionov, O.A., Fedotova, E.V., Kondratyeva, O.E., Dolchinkov, N.T., Kuznetsov, N.S. Actual and design wind loads for overhead transmission lines in the Central European part of Russia, *IOP Conference Series: Earth and Environmental Science* This link is disabled., 2023, 1281(1), 012050
- [36] L. Poiša, L. Antypova, Evaluation of the Effects of Herbicides on the Weeds and the Productivity of Hybrids Maize. *Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 14 th International Scientific and Practical Conference*, vol. 1, pp. 195–199, Jun. 2023, <https://doi.org/10.17770/etr2023vol1.7204>.
- [37] Stanchev G., Technical obstacles to speech intelligibility, *Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference* June 27-28, 2024, Vol. 3, pp 300-305
- [38] Simeonov M., M. Marinov, Determine the location of nodes in wireless sensor network by using genetic algorithm, *Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference* June 27-28, 2024, Vol. 2, <https://doi.org/10.17770/etr2024vol2.8059>, pp 247-252
- [39] V. Vasilev, D. Stefanova, and M. Icheva (2024). Green human resource management as a component of sustainable organizational development in environmental and natural economics, *ETR*, vol. 1, pp. 402–407, Jun. 2024, <https://doi.org/10.17770/etr2024vol1.7966>
- [40] Stefanova, D.P., Vasilev, V.P., Efremovski, I.P. (2023). Re-innovative organizational design: sustainable branding and effective communication - applied models in a world with new borders/without borders, Book Chapter: Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing, pp. 112–127; <https://doi.org/10.4018/978-1-6684-8681-8.ch006>
- [41] Dolchinkov N., . Construction Of A System For Monitoring The Pollution Of Water Bodies With Waste, *Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 15th International Scientific and Practical Conference*. Volume I, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2024vol1.7989>, pp 136-141
- [42] Dolchinkov N., Optimizing energy efficiency in the conditions of a global energy crisis, *Optimizing Energy Efficiency During a Global Energy Crisis*, 2023, ISBN13: 9798369304006 EISBN13: 9798369304013, <https://doi.org/10.4018/979-8-3693-0400-6>, pp. 1–9
- [43] Dolchinkov N., Karaivanova-Dolchinkova, B.E., Impact of Types of Electromagnetic Radiation on Living Nature, 14th International Scientific and Practical conference *Environment. Technology. Resources. Vide. Technology. Resursi*, 2023, ISSN 1691-5402, 1, pp. 55–59
- [44] Haralampiev M., Global environmental problems and their relationship with the protection of the population and infrastructure, Collection of reports from the scientific conference "Actual problems of the protection of the population and infrastructure", Vasil Levski, Veliko Tarnovo, 2012, volume 4 , pp. 34-49, ISBN 978-954-753-104-8;
- [45] Dolchinkov N., . Construction Of A System For Monitoring The Pollution Of Water Bodies With Waste, *Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 15th International Scientific and Practical Conference*. Volume I, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2024vol1.7989>, pp 136-141

Expectations and Opportunities for AI-enabled Systems Application in the Context of Military Communications and Cybersecurity

Angel Genchev

Bulgarian Defence Institute

“Prof. Tsvetan Lazarov”

Sofia, Bulgaria

a.genchev@di.mod.bg

ORCID: [0000-0002-0672-737X](https://orcid.org/0000-0002-0672-737X)

Emil Ivanov

Ministry of Defence

Sofia, Bulgaria

emotsiv@gmail.com

ORCID: [0000-0003-1658-9588](https://orcid.org/0000-0003-1658-9588)

Abstract—The rapid advancement of Artificial Intelligence (AI) is transforming military communications and cybersecurity by enabling higher levels of automation, adaptability, and data-driven decision-making. This paper examines the role of AI-enabled systems in military communication environments, with a focus on emerging operational trends, system requirements, and potential application areas. Particular attention is given to the effects of communication disruptions on mission effectiveness and to the growing need for resilient, secure, and interoperable communication infrastructures. The paper also outlines conceptual examples of AI-enabled military communication systems that can optimise network performance, prioritise critical data transmission, and strengthen cybersecurity through improved threat detection and response. The analysis shows that AI can significantly enhance situational awareness and real-time operational responsiveness, while also introducing new dependencies and implementation challenges. The study highlights the importance of adaptive system design and effective human-AI collaboration for the secure and reliable use of AI in military communications.

Keywords—artificial intelligence, command and control (C2), cybersecurity, military communications.

I. INTRODUCTION

Artificial intelligence (AI) has been developing at an incredible pace in recent years, impacting both civilian and military domains in ways that were difficult to predict in the past. The widespread availability of computing resources, vast libraries of open-source software, and large datasets has accelerated innovation and significantly reduced the difficulty of developing AI. As a result, AI technologies are no longer restricted to specialised actors but are increasingly accessible to a wide range of organisations, including potential adversaries [10], [11].

In the military domain, this shift is already visible. AI is being integrated into autonomous systems operating across air, land, sea, and cyber environments [12], enhancing capabilities such as multi-domain coordination,

sensor exploitation, and decision support. At the same time, recent conflicts suggest that these technologies contribute to a more complex and contested operational environment, where threats are not only more persistent but also harder to identify and counter.

This paper focuses specifically on digital military communications, which rely on interconnected networks, protocols, and distributed systems to enable command and control (C2), where human-machine interaction plays an increasingly important role [13], [15]. As modern operations become more dependent on timely and secure information exchange, communication systems evolve into both a critical enabler and a potential point of vulnerability.

The objective of this study is to analyse the expectations, requirements, and opportunities for applying AI-enabled systems in military communications and cybersecurity, while also identifying key risks associated with their integration. In practical terms, the goal is to outline how these technologies can improve operational effectiveness without introducing unacceptable levels of dependency or risk.

II. TRENDS IN THE MILITARY OPERATIONS

The integration of Artificial Intelligence into military operations is taking place in a rapidly evolving technological and regulatory environment. Although international discussions on the ethical and legal use of AI are ongoing, clear and enforceable frameworks are still limited. The absence of harmonised legal and ethical standards for military AI raises additional concerns regarding accountability, transparency, and the delegation of decision-making authority. In practice, this creates uncertainty, particularly in scenarios where adversaries may choose to employ AI capabilities without adhering to such constraints, including in the targeting of communication systems and cyber infrastructure.

One of the most noticeable developments in modern military operations is the increasing complexity of

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.75>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

communication systems. Unlike civilian networks, military communications are expected to function in contested and degraded environments, where infrastructure may be disrupted or deliberately attacked. Ensuring secure and reliable communication across geographically dispersed and often multinational forces remains a persistent challenge. This is further complicated by the need for interoperability between diverse technologies, ranging from terrestrial radio systems to satellite and data networks.

At the same time, military communication infrastructures are exposed to a continuously evolving cyber threat landscape [14]. Adversaries, including both state and non-state actors, employ a wide range of techniques such as advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, and targeted intrusion campaigns. These threats do not only aim to compromise data but can also disrupt critical services and degrade overall operational capability.

The growing dependence on digital technologies further amplifies these risks. Decision-making processes increasingly rely on large volumes of data from multiple sources, which introduces additional vulnerabilities related to data integrity and availability. In practice, a successful cyber attack may have cascading effects that extend beyond the cyber domain, affecting mission execution and even personnel safety.

In this context, Artificial Intelligence is increasingly seen as a practical enabler for improving the resilience and adaptability of military communication systems. By supporting faster anomaly detection, adaptive network management, and more effective response to cyber threats, AI addresses several of the key challenges associated with modern military operations.

These factors highlight the critical role of modern technologies, particularly Artificial Intelligence, in addressing the complexity of military communications.

III. REQUIREMENTS OF MILITARY COMMUNICATIONS

Military communication systems must satisfy a set of stringent and often competing requirements, driven by the dynamic and high-risk nature of military operations. These requirements extend beyond conventional communication system design and are closely linked to mission effectiveness, operational security, and decision-making processes.

A. Security and resilience.

Communication systems must ensure the confidentiality, integrity, and availability of transmitted information. This includes the use of advanced encryption techniques capable of withstanding sophisticated cyber threats, as well as mechanisms for detecting, resisting, and recovering from attacks such as jamming, interception, and intrusion. Resilience is particularly critical in contested environments, where partial system degradation must not lead to total communication failure.

B. Adaptability and flexibility.

Military communication networks must be capable of rapid reconfiguration in response to changing operational conditions. This includes dynamic routing, spectrum adaptation, and the ability to integrate new nodes or platforms in real time. Flexibility is essential for maintaining operational continuity in highly dynamic and unpredictable environments.

C. Interoperability.

Modern military operations often involve joint and multinational forces, requiring seamless communication across heterogeneous systems and platforms. Communication infrastructures must support interoperability between different technologies, standards, and protocols, enabling effective coordination and information exchange across domains.

D. Low latency and reliability.

Timely delivery of information is critical, particularly at the tactical level, where delays can directly impact operational outcomes. Communication systems must therefore provide reliable and low-latency data transmission, even under adverse conditions such as network congestion or partial infrastructure disruption.

E. Situational awareness.

Communication systems should support the generation of a coherent and accurate operational picture by integrating data from multiple sources. This includes sensor data, intelligence inputs, and system status information, presented in a form that supports rapid and informed decision-making.

These requirements highlight the need for advanced, adaptive, and intelligent communication solutions, where AI can play a central role in balancing performance, security, and operational effectiveness. They also imply that any disruption in communication systems may have critical operational consequences.

IV. IMPACT OF COMMUNICATION DISRUPTIONS

Communication disruptions in military operations can have immediate and severe consequences, directly affecting command and control processes and overall mission effectiveness. In highly dynamic and time-critical environments, even partial loss of communication may lead to delays in decision-making, reduced situational awareness, and loss of coordination between units. Such disruptions increase the risk of operational errors, including misinterpretation of commands, failure to execute critical tasks, or unintended engagement of friendly forces. In addition, the inability to maintain reliable communication can compromise operational security and expose vulnerabilities that adversaries may exploit.

From a strategic perspective, communication failures can degrade the effectiveness of entire operational frameworks, limiting the ability to coordinate actions across different domains and levels of command. In extreme cases, prolonged disruption may result in mission

failure, loss of critical assets, and increased risk to personnel.

Given the critical role of communication systems, ensuring their continuity, reliability, and protection against disruption is a fundamental requirement for modern military operations. This creates a strong need for intelligent and adaptive mechanisms capable of maintaining communication effectiveness under adverse conditions.

V. OPPORTUNITIES TO USE AI

In current military operational environments, where fast, secure, and reliable communication is critical, AI represents a key enabler for improving operational efficiency, resilience, and decision-making. AI-enabled systems can process large volumes of heterogeneous data in real time, which is particularly important in dynamic and uncertain conditions, supporting command and control (C2) processes.

One of the primary advantages of AI is its ability to enhance communication efficiency and adaptability. AI-driven network management can dynamically optimise routing, allocate bandwidth, and adapt to changing conditions such as interference, congestion, or partial infrastructure failure. This is particularly important in contested electromagnetic environments, where communication channels may be degraded or intermittently unavailable.

Another important advantage is the improvement of interoperability between different systems and units. By leveraging machine learning (ML) and natural language processing (NLP), AI can facilitate multilingual communication and support seamless interaction between multinational forces and heterogeneous platforms. From a cybersecurity perspective, AI provides advanced capabilities for detecting, analysing, and responding to threats. By continuously monitoring network traffic, system logs, and behavioural patterns, AI models can identify anomalies that may indicate malicious activity. Techniques such as behavioural analysis, deep learning, and anomaly detection enable early identification of cyber threats and support proactive defence mechanisms.

Adversarial AI techniques represent an emerging challenge, as malicious actors may manipulate input data or exploit vulnerabilities in AI models to degrade performance, evade detection, or influence decision-making processes.

In addition, AI supports automated threat assessment and response. AI-driven systems can classify incidents based on severity, origin, and potential impact, enabling faster and more efficient allocation of resources. Integration with incident response platforms allows the implementation of automated response actions, such as isolating compromised nodes, blocking malicious traffic, or initiating predefined mitigation procedures.

Another important application area is the optimisation and prioritisation of data transmission. In environments with limited bandwidth, AI can evaluate the relevance and

urgency of transmitted information, ensuring that critical data is delivered with priority. This is particularly relevant for sensor networks, where large volumes of raw data must be filtered and processed before transmission.

AI also enables the integration of communication and electronic warfare capabilities. By analysing the electromagnetic environment in real time, AI systems can optimise the performance of friendly communication systems while simultaneously minimising the effectiveness of adversary systems.

The role of AI varies across the different levels of military operations:

- **Tactical level.** AI systems support real-time operations by assisting personnel, enabling semi-autonomous actions, and enhancing situational awareness. Applications include autonomous platforms, swarm coordination, and adaptive sensor networks.

- **Operational level.** AI enables multi-sensor data fusion, situational assessment, and evaluation of alternative courses of action. It supports planning processes by optimising resource allocation and analysing different operational scenarios.

- **Strategic level.** AI can support long-term planning and decision-making by modelling complex scenarios, analysing adversary behaviour, and assessing the potential impact of different strategies. It may also contribute to information operations and influence activities in the information domain.

Despite these advantages, effective implementation of AI requires strong human–AI collaboration. While AI systems provide speed and analytical capabilities, human operators remain essential for contextual understanding, ethical judgment, and strategic decision-making [13, [15]. Practical implementation of AI-enabled systems in military environments also presents significant challenges. These include computational constraints at the tactical level, limited availability of representative training data, high requirements for model adaptation, and the need to ensure reliable performance under resource-constrained and adversarial conditions.

VI. CONCEPTUAL EXAMPLES OF AI-ENABLED MILITARY COMMUNICATION SYSTEMS

The application of Artificial Intelligence in military communications can be illustrated through several conceptual system models addressing key operational challenges. These concepts are aligned with the dynamics of the decision-making process, commonly described by the OODA loop [4], and reflect the differing requirements across tactical, operational, and strategic levels. Current developments in industry and research further demonstrate the continuous evolution of such systems [2], [3]. The effectiveness of communication systems at these levels depends on key performance characteristics, including latency, throughput, reliability, and security. While higher levels of command prioritise reliability and security, they can tolerate higher latency. In contrast, tactical-level operations require near real-time communication with strict

latency constraints. These differences define the appropriate technological approaches and optimisation strategies.

A. AI-based WAN optimisation model.

A conceptual AI-based WAN optimisation model with distributed agents is illustrated in Fig. 1.

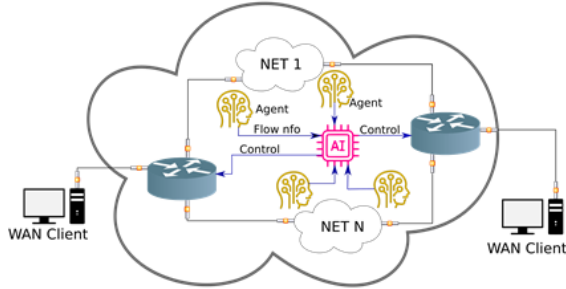


Fig. 1. AI-based WAN optimisation model

Network optimisation in tactical environments has traditionally relied on dynamic resource management and state estimation techniques [5], [6], followed by more advanced approaches such as software-defined networking and SD-WAN optimisation [7]. Building on these developments, a conceptual AI-based wide-area network (WAN) optimisation model can be constructed by integrating distributed monitoring agents and a central AI-based optimisation module. The agents collect real-time data on network conditions, including traffic load, delay, packet loss, and link availability. This information is transmitted via a management channel to an AI controller, which dynamically selects optimal routing paths and resource allocation strategies. Compared to traditional rule-based approaches, AI-driven optimisation enables predictive and adaptive behaviour, improving throughput and resilience under varying operational conditions.

B. AI-driven data filtering and prioritisation in sensor networks.

A conceptual network model, implementing an AI filter, is suggested in Fig. 2. It can be implemented as a component of a software-defined network similar to the separated planes network in [8].

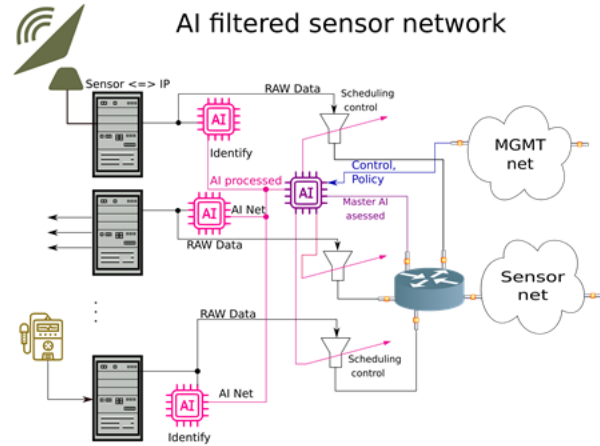


Fig. 2. Conceptual model of an AI-filtered sensor network

In bandwidth-constrained environments, efficient data transmission is a critical requirement. A conceptual model for AI-based filtering can be applied to sensor networks, where large volumes of raw data are continuously generated. In this model, AI modules embedded within sensor controllers analyse incoming data streams and determine their relevance based on learned patterns or predefined criteria. Only significant events, such as target detection, are prioritised for transmission. A higher-level AI controller aggregates these outputs and dynamically adjusts transmission priorities based on operational context and network conditions. This approach extends existing concepts of prioritised data handling and quality of service in distributed networks [8], enabling more intelligent and context-aware traffic management. It reduces unnecessary data transmission, optimises bandwidth utilisation, and ensures that critical information is delivered with minimal delay.

C. AI-enabled cybersecurity architecture.

A simplified diagram of the possible implementation of an AI-based solution to defend a network is presented in Fig. 3.

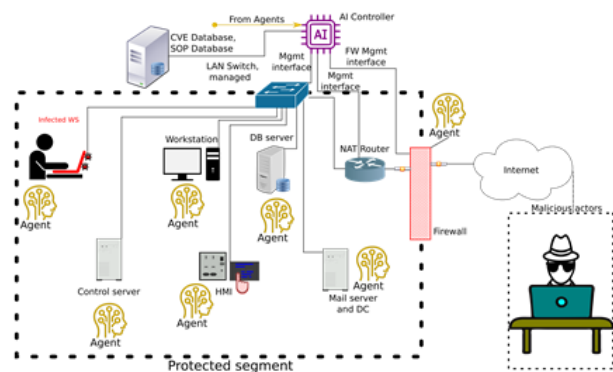


Fig. 3. AI-enabled conceptual model of a computer network

AI can also be integrated into communication systems to enhance cybersecurity through continuous monitoring, threat detection, and automated response. A conceptual architecture includes distributed monitoring agents

deployed across network nodes and a central AI controller responsible for assessment and control functions. Similar approaches have been explored in recent research and development efforts, including the AInception project [9], which investigates AI-driven and algorithmic solutions for automated network protection and response. In such architectures, the assessment component analyses network activity to classify behaviour as normal or malicious, while the control component determines appropriate response actions. These actions may include isolating compromised nodes, blocking malicious traffic, or alerting human operators. Different deployment strategies are possible, ranging from full agent distribution across all network devices to selective deployment at critical points such as routers, switches, and firewalls, each involving trade-offs between data availability, system complexity, and implementation cost.

These conceptual models demonstrate how AI can be embedded within military communication infrastructures to improve performance, efficiency, and security. While they are based on current technological capabilities and research trends, their practical implementation requires further validation in real-world operational environments.

VII. CONCLUSIONS

This paper examined the role of Artificial Intelligence in the context of military communications and cybersecurity, focusing on current operational trends, system requirements, and the impact of communication disruptions. The analysis highlighted the increasing complexity and vulnerability of modern military communication infrastructures, driven by their dependence on digital technologies and exposure to evolving cyber threats.

The study identified key opportunities for the application of AI, including adaptive network management, intelligent data prioritisation, enhanced situational awareness, and advanced cyber threat detection and response. These capabilities demonstrate the potential of AI to significantly improve the resilience, efficiency, and responsiveness of military communication systems.

In support of this analysis, three conceptual models were proposed, addressing AI-based WAN optimisation, intelligent sensor data filtering, and AI-enabled cybersecurity protection. These models illustrate how AI can be integrated across different layers of communication infrastructures to address both performance and security challenges. At the same time, the integration of AI introduces new challenges, including increased system complexity, dependence on data quality, and the need for reliable human-AI interaction. Ensuring transparency, robustness, and controllability of AI systems remains a

critical requirement for their effective deployment in military contexts.

Future research should focus on validating the proposed conceptual models through simulations, experimental environments, and operational scenarios, as well as assessing their performance under realistic communication and cybersecurity constraints.

Acknowledgements: The work in this paper has received funding from the European Union – European Defence Fund under GA no. 101103385 (AInception). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

REFERENCES

- [1] S. Prasad, D. Behl, J. Raju, and T. Lewis, "Building AI-driven closed-loop automation systems," IBM Developer, [Online]. Available: <https://developer.ibm.com/articles/an-introduction-to-closed-loop-automation/>.
- [2] Thales Group, "Tactical networks," [Online]. Available: <https://www.thalesgroup.com/en/markets/defence-and-security/mission-critical-communications/tactical-networks>.
- [3] General Dynamics Mission Systems, "Warfighter Information Network-Tactical (WIN-T)," [Online]. Available: <https://gdmissionsystems.com/communications/warfighter-information-network-tactical>.
- [4] L. M. Blaha, "Interactive OODA Processes for Operational Joint Human-Machine Intelligence," in STO-MP-IST-160, pp. 3–18.
- [5] A. S. Peng, D. M. Moen, T. He, and D. J. Lilja, "Automatic Dynamic Resource Management Architecture in Tactical Network Environments."
- [6] R. Fronteddu et al., "State Estimation for Tactical Networks: Challenges and Approaches," in MILCOM 2018, pp. 1042–1048, doi:10.1109/MILCOM.2018.8599823.
- [7] VMware, "SD-WAN Dynamic Multipath Optimization," [Online]. Available: <https://kb.vmware.com/s/article/2733094>.
- [8] C. Gedo et al., "GIG QoS Inter-Domain Interoperability Challenges," in MILCOM 2007, <https://doi.org/10.1109/MILCOM.2007.4455023>.
- [9] AInception Project, "Project overview," [Online]. Available: <https://www.ainception.eu/overview>.
- [10] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.
- [11] NATO STO, "Artificial Intelligence and Autonomy in Defence," Science & Technology Organization, 2020.
- [12] P. Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Company, 2018.
- [13] M. Lewis et al., "Human-Machine Teaming for Military Decision Making," IEEE Computer, vol. 51, no. 12, pp. 38–45, 2018.
- [14] ENISA, "Artificial Intelligence Cybersecurity Challenges," European Union Agency for Cybersecurity, 2021.
- [15] J. Kott and C. Arnold, "The Promises and Challenges of AI for Military Decision-Making," Military Operations Research, 2019.

An Integrated Concept for the Protection of Photographic and Electronic Equipment during Crime Scene Investigation Using a Risk-Oriented Protocol

Georgi Georgiev

*Department of Security and Safety
Varna Free University "Chernorizets Hrabar"
Varna, Bulgaria
georgi.georgiev@vfu.bg*

Stefko Burdzhiev

*Department of Security and Safety
Varna Free University "Chernorizets Hrabar"
Varna, Bulgaria
stefko.burdzhiev@vfu.bg*

Abstract—Forensic photography is performed in uncontrolled environments where photographic and other devices are exposed to both direct impacts (blood and body fluids, dust/soot, chemical residues, water, mechanical impacts) and indirect risks, turning the equipment into a reservoir and a means of transferring traces and contamination between objects, different areas and subsequent examinations. Typically, personal protective equipment (PPE) is considered as a barrier to protect personnel, but the same barrier logic can be symmetrically applied to equipment through different layers of protective coatings, touch interface control, zoning (HOT/WARM/COLD), role separation, sealing before transport and staged decontamination. This report proposes a protocol that combines physical contamination control with digital integrity control (metadata, controlled transfer, hashing) so that images and devices are processed in a defensible manner within the framework of quality management.

Keywords—crime scene investigation, equipment protection, forensic photography, personal protective equipment.

I. INTRODUCTION

Photographic documentation is a fundamental mechanism for capturing traces and ensuring subsequent verifiability of what is described in the protocols for inspection of crime scenes, measurements and reconstruction. The expansion of photographic practices with 360° panoramas, photogrammetry, and multispectral studies using alternative light sources (ALS), drones and portable 3D scanners increases the number of devices that are introduced and removed from potentially hazardous and contaminated environments.

There are two interrelated groups of risks. First, uncontrolled exposure to biological fluids, unknown powders, soot, solutions and corrosive residues can lead to damage to optical coatings, rubber seals, adhesive joints and electrical connectors, which can compromise the performance of the equipment. Second, the equipment (especially the camera and accessories) is subject to repeated handling by the operator and can thus come into contact with surfaces carrying biological material, fibres or particles. Without proper control, the devices can carry traces between different areas, in packing areas, in official police vehicle, or when moving to subsequent examination of evidence. In private cases, the camera itself can become a real source of unknown deoxyribonucleic acid (DNA).

The purpose of this report is protection of the reliability and operational readiness of equipment and protection of evidentiary integrity by minimizing cross-contamination. This paper contributes a risk-oriented protocol that applies personal protective equipment (PPE) principles - barrier protection, touch-interface control, procedural standardization, and traceability - to photographic and electronic equipment used for Crime Scene Investigation (CSI).

Original contributions of this paper are:

- A risk-oriented protocol that symmetrically applies PPE principles to photographic and electronic CSI equipment.
- A combined zoning-and-state model for equipment (COLD/WARM/HOT; CLEAN, IN-USE-HOT, QUARANTINE,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.117>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

DECONTAMINATED) linked to role separation.

- Touchpoint-based interface control with observable glove-change triggers to reduce cross-contamination during imaging.
- An integrated workflow that couples physical contamination control with digital integrity controls (controlled transfer, hashing, and audit logs).

A. Related Research and Good Practices

Experimental studies in forensic science have shown that practitioners can transfer DNA to simulated scenes, and the use of protective clothing reduces the potential for contamination, which could serve as a basis for studying barrier-oriented crime scene examination practices [1].

Regulatory and best practices in DNA contamination control emphasize preventive measures to limit access, zoning, route control, routine glove changes, and clear separation of sterile supplies/equipment from seized objects during transport [2]. This applies to cameras, tripods, and lighting, which remain implicitly included in many standard operating procedures (SOPs) but are rarely formalized as a set of risky touchpoints and equipment conditions.

Additionally, good practices in digital forensics and digital evidence management emphasize documented workflows and integrity checks (e.g., hash functions) for demonstrable file integrity. Therefore, a defensible imaging workflow requires both physical contamination control and digital integrity control [3, 4].

B. Regulatory and Methodological Framework

In the European Union (EU) context, PPE should comply with the requirements of Regulation (EU) 2016/425 on essential health and safety requirements, conformity assessment and instructions for use [5]. For forensic examinations and work, European Network of Forensic Science Institutes (ENFSI) guidance documents define functional areas and infrastructure (material storage, changing room, evidence area) supporting the controlled circulation of equipment around the scene [6]. DNA contamination guidelines (e.g. FSR-GUI-0016) frame controls as a combination of prevention and detection through appropriate PPE, restricted access and effective separation of equipment/consumables from seized objects during transport and processing [2]. The standard of International Organization for Standardization (ISO) 18385 defines requirements for products used for the collection, packaging and storage of biological material, in order to minimize contamination with human DNA. Although the standard is aimed at single-use products, its logic supports similar approaches for reusable devices - standardized interfaces, limited uncontrolled contact, and documented cleaning steps [7]. Operationally, the sequences for donning/doffing PPE and the management of contaminated surfaces are well described in health protocols and can be adapted to forensic crime scene

examinations, taking into account the specific risks of the particular case [8].

II. MATERIALS AND METHODS

A. PPE Categories And Controlled Donning/Doffing Relative To Electronic Equipment

For the purposes of scene documentation, PPE should be understood as a layered system rather than as a single garment. Basic hand protection is provided by disposable nitrile gloves, which are the primary barrier against direct transfer of biological material and particulate contamination. Respiratory protection ranges from simple masks used for nuisance dust control to filtering facepiece class 2/filtering facepiece class 3 (FFP2/FFP3) respirators when aerosols, soot, or unknown powders may be present. Eye and face protection includes goggles or face shields when splashes, flying particles, or intensive alternate light source/ultraviolet (ALS/UV) work are expected. Body protection may include disposable coveralls, sleeves or aprons, while footwear protection includes dedicated work shoes and disposable overshoes where transfer from the floor surface is a realistic risk [5], [2], [8].

From the standpoint of photographic and electronic equipment, not all PPE elements have the same operational significance. Gloves directly affect camera handling, button sensitivity and touchpoint transfer, masks and respirators influence communication and the risk of exhaled contamination near optical devices. Goggles and face shields affect viewfinder use and the handling of optical filters, coveralls and sleeves affect the risk of brushing against tripods, light stands and evidence markers. This functional distinction is useful because it links PPE selection not only to worker protection, but also to the quality and cleanliness of device operation within the evidential environment [6], [2], [4].

A controlled donning sequence is necessary because the first uncontrolled contact often occurs before the team enters the HOT zone. As a rule, inner PPE elements that are intended to remain with the operator for the whole task should be donned first, followed by body protection, footwear protection, respiratory protection, eye protection, and finally the outer glove layer. The outermost glove layer should be the last element applied [8].

Electronic equipment should not be handled at every stage of donning. The recommended approach is to divide contact into three moments - pre-donning preparation of the kit in a CLEAN condition, a final functional check after the main PPE ensemble has been donned but before the outer gloves have touched contaminated surroundings and operational handling only after entry under the selected control level. In practice, batteries, memory cards, lens mounting, time synchronization and cover placement should be completed in COLD zone before the outer gloves are exposed. After that point, the equipment is treated as a controlled clean object whose status must be preserved until scene work begins.

The handling of electronic equipment can be organized into distinct operational stages. Stage 1 is pre-entry

preparation in COLD, where devices are assembled, labelled, synchronized and protected. Stage 2 is controlled transition through the access point, where only essential confirmation actions are allowed. Stage 3 is active use in HOT, where the operator should touch only the minimal exposed interface and avoid unnecessary adjustment cycles. Stage 4 is WARM-zone stabilization, where covers, outer bags and visible contamination status are managed. Stage 5 is post-scene handling in COLD, where media transfer, logging and secondary decontamination take place. This stage model helps maintain a consistent relation between PPE status, zone status and equipment status.

Such staging also clarifies when glove changes are required. For example, gloves used to move markers, touch doors, assist with object manipulation or contact wet/dirty surfaces should not be used for detailed manipulation of the camera interface without replacement. Conversely, when a camera-only glove policy is adopted, the operator can preserve a more stable clean-touch condition for image acquisition while the evidence handler performs higher-risk contact tasks. This reduces ambiguity in the field and strengthens the procedural defensibility of the workflow [2], [7].

The sequence for removing PPE is as important as the sequence for donning it because contaminated outer layers can transfer material back to the operator, the vehicle and the equipment if they are removed in an uncontrolled order. As a general principle, the most contaminated external elements are removed first in the transition area, while the inner layers that protect the operator during the final handling stages are removed later. Outer gloves used in HOT should therefore be removed or exchanged before touching clean storage areas, digital work surfaces, keyboards, packaging materials or the inner compartments of transport cases [2], [8].

After leaving HOT, the device should first be isolated or quarantined before progressive doffing continues. This prevents the common error of placing a possibly contaminated camera or tripod into a nominally clean area while the operator is still partially contaminated. Only after the device has been bagged or stabilized should the sequence proceed through removal of disposable sleeves or coveralls, eye/face protection and respirators in accordance with local safety rules, with hand hygiene or glove replacement inserted whenever the procedure crosses from dirty-touch to clean-touch actions. The key methodological point is that doffing and equipment handling should be read as one integrated chain rather than as two separate tasks.

B. Threat Model and Design Requirements

Hazards are grouped as biological (blood, body fluids, decomposition), dust particles (dust, soot, fingerprint powders, fibres), chemical (solvents, acids/bases, synthesis lab residues, scene cleaning agents), physical-mechanical (impacts, water, temperature differences, vibrations), optical (ALS/UV/laser sources, glare and risk of filter/sensor degradation). Each group generates simultaneously a risk to personnel, a risk to evidentiary integrity through transfer/contamination and a risk to the

functionality of the equipment through corrosion, dusting or damage.

Each hazard group should be assessed not only by its direct effect on personnel but also by the type of secondary contamination it can generate on equipment surfaces. Biological contamination has the highest evidential sensitivity because even minimal uncontrolled contact may later be interpreted as scene-derived material. Dust, soot, and powder hazards are especially relevant because they persist in recesses, controls, and textile components and are easily redistributed during packing, transport, and later reuse of the equipment.

The most common pathways occur through repeated touch points such as the shutter release, command dials, rear display, viewfinder/eyecups, lens barrel/focus ring, quick release plate, strap/harness, and tripod controls. Paths are activated when transitioning between “dirty” activities (marking, moving objects, surface testing) and “clean” activities such as packaging, filling out protocols, and working with files. Without rules for changing gloves and interface management, the risk of trace transfer is high.

Before entering the scene, the team should mark the specific parts of the equipment that will be touched during work. For the camera, these usually include the shutter release, command dials, rear screen, memory-card door, battery compartment, grip, and lens barrel; for the tripod, the leg locks, centre column, and quick-release plate; for the flash or ALS device, the control buttons and mounting points; for the tablet, the screen, case edges, and ports; and for the transport case, the handle, latches, and inner compartments. Each of these points should be assigned to one of three categories - surfaces that may be touched with clean gloves, surfaces that may be touched only after glove change, and surfaces that must remain protected and should not be handled inside the HOT zone unless strictly necessary. In this way, contamination control is linked to real manipulations rather than to general warnings. The map also makes it easier to justify, document, and later explain why certain covers were applied, why gloves had to be changed at specific moments, and why some operations were restricted to the WARM or COLD zone.

The criteria used to evaluate and select PPE and equipment-protection measures during scene work are:

- conducting a risk assessment to select an appropriate barrier with sufficient resistance to the identified hazards;
- operational compatibility (PPE must enable safe work and ergonomics for operating the camera and optics);
- possibility of decontamination and material compatibility (cleaning agents must not damage coatings/seals);
- traceability and auditability (logs, labelling of equipment states) - information must be sufficient to reproduce the process;

- evidence-friendly materials - covers/adhesives must not shed fibres and must not leave residues that could be interpreted as traces.

Taken together, these criteria form a practical selection matrix rather than a purely descriptive list. In field deployment, the team should be able to justify why a given barrier was chosen, why another material was rejected, and whether the selected solution prioritizes operator dexterity, contamination control, equipment preservation, or a balanced combination of the three. This makes the protocol auditable and links equipment protection measures directly to the logic of risk assessment already used for PPE selection.

C. Risk Assessment and Control Levels

To improve consistency and reproducibility, the qualitative assessment is operationalized with simple quantitative indicators. In Table 1, Severity (S) and likelihood (L) are scored on ordinal 1–5 scales for both occupational risk and evidentiary (cross-contamination) risk.

TABLE 1. ORDINAL SCORING SCALES USED IN THE RISK ASSESSMENT.

Score	Severity (S) – example interpretation	Likelihood (L) – example interpretation
1	Negligible exposure, no visible contamination; minimal contact surfaces	Rare, unlikely in this scene context
2	Minor localized exposure, limited residues, short contact	Unlikely but plausible
3	Moderate exposure, repeated handling, detectable residues or dust/soot	Possible under normal operations
4	High exposure, wet biofluids/powders, frequent contact and handling	Likely, expected during task
5	Very high exposure, unknown/highly hazardous residues, sustained contact or aerosolization	Almost certain, multiple triggers present

Risk scores are computed as:

$$R_{occ} = S_{occ} * L_{occ}, \quad (1)$$

$$R_{evid} = S_{evid} * L_{evid}, \quad (2)$$

and the control level is determined by

$$R = \max(R_{occ}, R_{evid}). \quad (3)$$

A practical thresholding scheme is L1 ($R \leq 6$), L2 ($8 \leq R \leq 12$), and L3 ($R \geq 15$), with escalation when unknown substances are suspected.

Field solutions require a rapid method. A two-axis assessment in Table 2 is proposed - severity and probability are assessed for occupational risk and evidentiary risk, with the higher score determining the level of control. Levels L1–L3 are tailored to the reality of forensic teams without a dedicated hazardous materials (HazMat) resource, but

allow for escalation when unknown substances are suspected.

TABLE 2 RISK-BASED CONTROL LEVELS

L e v e l	Typical environment	PPE (personnel)	Equipment package	Key rules
L 1	Low bio/dust risk, indoor areas with no visible contamination	Gloves (nitrile), shoe covers as needed, mask when dust is present	Basic protective kit – camera cover, UV/clear filter, dedicated clean wipes	Change gloves when transitioning to camera handling so that the equipment remains in a “clean state”
L 2	Moderate risk: localized blood/bio fluids, dust/soot, fingerprint powder	Double gloves; FFP2/3 respirator when aerosols are possible, protective goggles	Layered barrier package – disposable covers for grip/display, protective bags for accessories, dedicated straps	HOT/WARM/COLD, separate camera operator from evidence handler, controlled touchpoints
L 3	High/unknown risk: decomposition, unknown powders, chemical residues	Extended PPE according to risk, mandatory zoning and supervised doffing	Maximum barrier – full camera/lens coverage, sealed transport containers, segregated batteries/cards	Staged decontamination, prohibition on opening cases in the HOT zone, and documentation of every manipulation

The selected level is documented in the crime scene report. Where feasible, engineering and organizational measures (ventilation, restricted access, controlled movement trajectory) are applied before increasing protection through PPE.

The assessment should remain dynamic throughout the inspection. Escalation is required when the team encounters previously unknown powders, wider biological spread than initially visible, wet surfaces, active cleaning chemicals, or the need for close-range imaging that increases contact risk. De-escalation is possible only after the scene sector has been re-evaluated and the rationale has been recorded. In this way, control level becomes a managed operational variable rather than a one-time label assigned at the start of the examination.

D. Zoning, Roles, Equipment States and Separation During Transport

Zoning as shown on Fig.1 aims to reduce uncontrolled movement and the transfer of trace material:

- COLD includes a command area and a changing area where devices are prepared and settings are checked;
- WARM serves as a controlled transition zone with waste and decontamination points;

- HOT is the active scene area. Entry/exit points are minimized and a record is kept of persons and equipment passing through them [2,7].

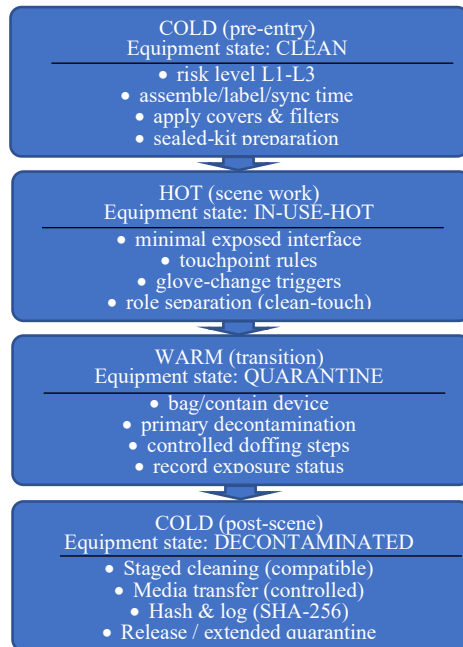


Fig. 1. Operational stages.

The protocol recommends operational role separation - a camera/scanner operator (“clean-touch” role) to minimize contact with items/traces, and an evidence handler (“dirty-touch” role). Equipment is treated as being in one of the following states - CLEAN (prepared/covered), IN-USE-HOT (used in HOT), QUARANTINE (for transport to decontamination), DECONTAMINATED (restored for COLD). All transitions between zones, operational phases, and equipment states should be documented in the crime scene inspection report.

When various reasons do not permit two separate experts, the same person may alternate between the roles only under explicit transition rules - a pause in activity, glove change, confirmation that no seized object is being handled simultaneously, and recording of the equipment state before the next action. This fallback rule is important for small field teams because it preserves the logic of separation even when personnel resources are limited, and it prevents the protocol from becoming impractical outside large forensic units.

A common weakness is the linking of different environments via service vehicles. Separation into a clean and a dirty container is recommended - CLEAN contains unopened consumables and covered devices, whereas DIRTY contains seized items and used equipment pending decontamination. Transfer between compartments is prohibited without decontamination step [2].

E. Equipment Protection Design

Protection is implemented as a layered system - an outer cover, local disposable interfaces for high-frequency touchpoints (grip, buttons, display), and an internal clean

zone for batteries/cards. The goal is to reduce the surface area of uncontrolled contact and to facilitate replacement of the most contaminated layer without interrupting operations.

The layered approach is scientifically useful the outer layer receives the highest burden and can be removed or replaced without exposing the underlying controls, while local interface covers confine contamination to the limited surfaces actually touched during image acquisition. This reduces the decontamination burden, shortens recovery time after scene work, and makes it easier to explain which parts of the device were potentially exposed and which parts remained protected throughout the operation.

Covers must be impermeable to bio fluids at a level consistent with L2–L3 while also being low-lint. Smooth materials that do not shed fibres and do not crumble under friction are recommended. In dust/soot environments, it is critical to limit openings around the lens mount and rings and to use a protective (clear/UV) filter to protect the front element.

One of the most effective yet underestimated controls is glove management. At L2–L3, the use of two glove layers (inner + outer) with frequent replacement of the outer layer is recommended. Practical triggers for glove change include touching an item/surface in HOT zone, using markers/scales, contact with wet/sticky areas, transitioning to packaging/media handling, and before touching the main camera touchpoints (shutter release, dials, display). A camera-only outer-glove concept is also possible, where the outer gloves are used only to operate the camera and are replaced when leaving HOT zone.

To make this rule operational, glove-change events should be tied to clearly observable triggers rather than left to individual judgment alone. The protocol therefore benefits from predefined change points before camera activation, after evidence contact, after marking or measuring, before touching batteries or memory cards, and before returning to the transport container. This approach reduces inconsistency between operators and creates a repeatable sequence that can be taught, supervised, and later reconstructed if contamination concerns are raised.

Tripods and lighting devices have large surfaces and mechanical joints (locks, sections) that are difficult to decontaminate. Disposable covers for handles/locking levers are recommended, as well as separation into a dirty tripod for HOT and a clean tripod for COLD/WARM zones. All cables and adapters should be kept in sealed, clean polyethylene bags. For ALS/UV devices, controls include management of optical filters and protection from dust, and a procedure to avoid cross-touching between filters/goggles and camera operation.

From an engineering perspective, these accessories should be treated as separate contamination objects rather than as neutral extensions of the camera. Dedicated HOT-zone accessories are preferable whenever resources allow, because locks, telescopic sections, light stands, and filter holders accumulate particulate material in areas that are

difficult to inspect visually. The same logic applies to ALS goggles and optical filters.

Mobile devices are high-risk due to frequent contact, heat, and difficult-to-clean areas around ports. Therefore, replaceable protective cases, disposable transparent conductive screen films, and dedicated clean styluses for COLD/WARM use are recommended. For 3D scanners, a clear policy on surface contact, defined placement locations (clean pads), and separate transport bags/containers are required.

Equipment is carried in pre-prepared ('sealed') kits with a tamper-evident outer layer. In the HOT zone, common cases are not opened except when necessary. Instead, individual bags/containers are used for each device. This reduces the risk of contaminating the entire kit and improves traceability.

F. Operational Workflow

COLD performs battery/card checks, time synchronization, pre-set shooting profiles, attachment of protective filters and covers, marking of the kit (camera/lens ID), and recording of the initial state (CLEAN). Separate bags are prepared for used covers and waste. This preparatory step supports standardized on-scene evidence handling and preservation workflows [9].

This preparatory stage is also the correct place to define the expected photography sequence, the probable need for lens changes, and the threshold for bringing additional accessories into the scene. By making these decisions before entry, the team reduces ad hoc opening of cases in contaminated areas and limits unnecessary manipulations. Pre-entry preparation therefore has both a logistical function and a contamination-control function, because the number of later interventions strongly influences the total exposure burden of the equipment.

Entry into HOT is via a controlled access point. The camera operator should maintain minimal contact with items and surfaces. If a lens change is required, it is performed in WARM, where a clean pad and a controlled procedure are provided (change outer gloves, minimize the time the mount is exposed, immediately close and cover).

When leaving HOT, the device is placed into an outer bag/container (quarantine). In WARM, primary decontamination of the outer cover surfaces (if applicable) is performed and outer gloves are removed in a controlled manner to avoid contaminating clean zones.

In COLD, media are removed/transferred in accordance with the digital policy, secondary decontamination of the device is performed (after removing the covers), and the state is returned to DECONTAMINATED. If chemical/biological contamination is suspected, extended quarantine and consultation with competent units are provided.

G. Decontamination and Material Compatibility

Decontamination should be effective against the identified hazard while preserving the functionality of the device. A mechanical first, then chemical approach is

recommended. The goal is to remove dust/particles with lint-free cloths and appropriate agents before using solutions. No liquids are allowed to enter ports and connectors. Minimal amounts of disinfectants are used for this, and controlled drying is also performed.

Cleaning actions should proceed from the least sensitive and least contaminated external surfaces toward the most sensitive interfaces, while avoiding repeated wiping that can spread residues into seams and controls. The selected cleaning agent, concentration where applicable, contact time, and any visible adverse effect should be recorded whenever the contamination event is significant.

Optical coatings and seals can be sensitive to solvents and aggressive agents. Therefore, the protocol includes using manufacturer-approved optical cleaners, avoiding acetone/strong solvents on plastics and rubber parts, and pre-installing a protective filter that is replaced/cleaned separately in the event of accidental contamination. At L3, if unknown chemicals are present, isolation and assessment prior to cleaning is preferred.

For tripods and lighting, modular approaches are used using replaceable disposable grip covers and locking levers, sealed cable bags, and separate HOT zone kits. In case of heavy contamination, disposable interfaces are preferred over aggressive chemical cleaning, which can leave residue or pose a risk to the image.

H. Digital Control of Image Integrity

To make processing defensible, the principle of minimal intervention is followed. Original files are preserved unchanged, and processing is carried out on copies. In the COLD zone, the camera/card identifier, time synchronization, file sequence, and transfer conditions are documented. The use of write-blocker devices is recommended when working with media where applicable, as well as limiting automatic editing/compression functions.

When transferring images, cryptographic hashes (e.g., SHA-256) are computed for original files and/or archives and recorded in a log. The log includes date/time, operator, source, destination, tool used, and the resulting hash values. This reduces the risk of disputes about data manipulation and complements the physical traceability of equipment.[3]

To reduce errors and contamination of the work environment, role separation is recommended: the camera operator should not simultaneously handle media processing in HOT/WARM zones. Digital processing is performed in a clean area using separate gloves or after sanitizing hands and the work surface.

Therefore, a defensible digital chain of custody should include a minimal but structured record consisting of device identifier, memory card identifier, operator, transfer workstation, transfer date and time, hash values, storage destination, and any subsequent export or processing action. When these data are linked the result is a unified traceability model in which the same device is controlled

both as a potential carrier of scene contamination and as the source of evidential image files.

I. Scenario Based Application of the Protocol

In Blood Scene/Biological Fluids (L2), the key measures include double gloves with frequent replacement of the outer layer, full camera cover, a protective filter, prohibition on placing the camera/tripod on the floor without protective pads in the HOT zone, quarantining the device when exiting, and staged decontamination. In addition, a protected area for memory card/battery changes is provided in the WARM zone.

For soot and dust, emphasis is placed on particulate control - covers with minimal openings are used, respiratory protection is worn when aerosols are possible, and mechanical cleaning is performed before using liquids. To prevent abrasion, lint-free wipes, photographic brushes, and air blowers are used, while avoiding dry rubbing on optical surfaces.

For unknown substances (unknown powders/chemical residues (L3)), the protocol prioritizes isolation and assessment, restricted access, maximum equipment barrier, sealing during transport, and postponing aggressive cleaning until the hazard has been identified. If needed, coordination with competent units for HazMat assessment is initiated.

In such situations, the protocol should explicitly allow tactical limitation of photographic actions until safe conditions are established. In other words, not every technically possible close-up should be attempted immediately if the action would require opening cases, changing optics, or bringing additional devices into a potentially hazardous zone.

III. RESULTS AND DISCUSSION

A. Practical Limitations and Implementation Considerations

Key practical limitations and trade-offs include:

- Dexterity versus barrier strength - thicker gloves improve protection but may increase the probability of equipment drops and control errors.
- Material compatibility - cleaning agents and disinfectants must be compatible with optical coatings, rubber seals, plastics, and adhesives, manufacturer guidance should be followed.
- Small team constraints - role separation (clean-touch vs dirty-touch) may be infeasible, in such cases, explicit transition rules and glove-change checkpoints are required.
- HazMat boundary - the protocol does not replace specialist hazardous-material procedures, for unknown powders/chemicals, escalation and isolation remain mandatory.

- Environmental stressors - rain, condensation, low temperatures, and dust storms may require additional protective layers and can limit decontamination options on scene.
- Consumable availability and cost - sealed kits and disposable interfaces reduce risk but require logistics and procurement planning.

The protocol is applicable as an upgrade to existing inspection SOPs, without requiring expensive equipment. The main investment is organizational, through standard kits, barrier/interface consumables, and training. The choice of materials should take into account 'evidence-friendliness', lack of release fibres, and controllable adhesives.

In the context of technically oriented protection from exposure to hazardous substances, the contribution is positioned as an 'engineering' systematization of barrier controls for device reliability and evidentiary integrity. This allows to argue the technological and managerial value of the protocol and its transferability to other field activities (emergency and rescue operations, critical infrastructure inspections).

B. Comparison to Existing Standards and Added Value

Table 3 maps the proposed protocol to existing guidance and standards and highlights the added value for photographic/electronic CSI equipment.

Table 3. Mapping to standards/guidance and added value of the proposed protocol.

Source	What it already covers	Gap for CSI equipment	Added value in this paper
Regulation (EU) 2016/425 [5]	PPE conformity and essential safety requirements for personnel	Does not specify protection/handling of reusable documentation equipment	Extends barrier logic from personnel to equipment and defines equipment states and packaging controls
ENFSI BPM-SOC [6]	Scene organization, functional areas, access and workflow principles	Limited operational detail for camera/ALS/tripod touchpoints and kit segregation	Formalizes zoning + equipment-state transitions and role separation for clean-touch imaging
FSR-GUI-0016 [2]	Contamination controls: access restriction, separation of sterile supplies from seized items	Equipment treated implicitly; lacks interface-level controls and staging rules	Introduces touchpoint mapping, glove-change triggers, sealed-kit philosophy, and staged decontamination
ISO 18385 [7]	Minimizing human DNA contamination for consumables	Not aimed at reusable devices; no operational workflow for cameras/scanners	Transfers 'forensic DNA grade' logic to reusable device interfaces and

	and packaging		cleaning/verification steps
SWGDE imagery integrity guidance [3]	Principles for maintaining integrity of imagery and workflows	Does not address physical scene contamination or equipment as trace carrier	Couples digital integrity (hash/log) with physical contamination control in one protocol

C. Sequential Summary Procedure

Before entry, the team assigns operational roles, selects the control level, prepares the camera kit in a documented CLEAN state, applies covers and protective filters, synchronizes time, and decides which accessories are genuinely necessary for the planned imaging tasks.

The sequence begins with controlled donning - the main PPE ensemble is completed in COLD, the outer glove layer is applied last, and only then is the final equipment check performed. This ensures that the first operational contact with the camera kit occurs under a known barrier condition and that subsequent glove changes can be tied to clearly defined transitions between clean-touch and dirty-touch tasks.

At the entrance to the scene, the operator confirms the transition into HOT/WARM/COLD logic, records the equipment identifier, and ensures that transport cases containing reserve items remain outside the contaminated area unless a justified operational need arises.

Inside HOT, image acquisition is performed under the principle of minimal exposed interface. Only the necessary controls are touched, the device is not placed on uncontrolled surfaces without a barrier, and glove changes are performed at predetermined trigger points rather than irregularly.

When tripod, ALS, flash, tablet, or scanner systems are used, each accessory is handled as a separate contamination object with its own covers, placement rules, and post-use packaging. This prevents the camera protocol from being undermined by inadequately controlled supporting equipment.

If operational demands change, such as the need for macro imaging, lens replacement, or movement into a more heavily contaminated sector, the control level is re-evaluated and the transition is documented before work continues.

On leaving HOT, the device enters quarantine in an outer bag or container. In WARM, the team removes or stabilizes the most contaminated outer layers, records exposure status, and prevents cross-contact between used barriers, clean consumables, and transport compartments.

In COLD, memory media are handled under the digital integrity policy, original files are transferred without alteration, hashes are generated and recorded, and the linkage between image files, device identifier, operator, and transfer event is preserved in a single log structure. To avoid contamination of memory cards and other equipment during hashing, they can be sealed in clean packaging and

hashing and copying can be performed in laboratory conditions.

Secondary decontamination is then performed with agents and methods compatible with the actual material and hazard profile of the device. After inspection for residual contamination or damage, the equipment is either returned to DECONTAMINATED status or retained in extended quarantine for further assessment.

The procedure ends only when both chains are complete. The physical chain showing where the equipment moved and how it was protected, and the digital chain showing how the files were preserved, transferred, and verified. This combined closure is the core methodological contribution of the proposed protocol.

IV. CONCLUSION

An integrated protocol for the protection of photographic and electronic equipment during crime scene investigation is proposed, which treats the devices as contamination-sensitive elements rather than as neutral instruments. Through risk-based levels of control, zoning, role separation, layered barriers for equipment, staged decontamination, and traceable digital integrity control, the protocol reduces the risk of trace material transfer and equipment damage. The expected result is increased reliability in documentation and more consistent quality of work during investigations in different operational scenarios.

REFERENCES

- [1] G. N. Rutt, A. Hopwood, and V. Tucker, "The effectiveness of protective clothing in the reduction of potential DNA contamination of the scene of crime," *International Journal of Legal Medicine*, vol. 117, no. 3, pp. 170–174, Jun. 2003, <https://doi.org/10.1007/s00414-002-0348-1>.
- [2] Forensic Science Regulator, Guidance: Contamination Controls – Scene of Crime, FSR-GUI-0016, Issue 1, Oct. 2023.
- [3] Scientific Working Group on Digital Evidence, Best Practices for Maintaining the Integrity of Imagery, 17-I-001-1.1, Mar. 3, 2025.
- [4] ISO/IEC 17025:2017, General Requirements for the Competence of Testing and Calibration Laboratories, 2017.
- [5] European Parliament and the Council of the European Union, "Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC," *Official Journal of the European Union*, L 81, pp. 51–98, Mar. 31, 2016.
- [6] ENFSI, Best Practice Manual for Scene of Crime Examination, ENFSI-BPM-SOC-01, ver. 01, Nov. 2021.
- [7] ISO 18385:2016, Minimizing the Risk of Human DNA Contamination in Products Used to Collect, Store and Analyse Biological Material for Forensic Purposes — Requirements, 1st ed., 2016.
- [8] Centers for Disease Control and Prevention, "Sequence for Putting on Personal Protective Equipment (PPE)," poster. [Online]. Available: <https://www.cdc.gov/infection-control/media/pdfs/Toolkits-PPE-Sequence-P.pdf>. Accessed: February 21, 2026.
- [9] Organization of Scientific Area Committees (OSAC) for Forensic Science, Standard for On-Scene Collection and Preservation of Physical Evidence, OSAC 2021-N-0018, Mar. 2021.

Leadership Expectations across Strategic, Operational, and Tactical C2 Levels in a Hypothetical Military Operation: The Influence of Procedural Justice, Trust in Leaders, and Digitalization in Peacetime Settings

Teodora Georgieva

Rakovski National Defence College
Defense Advanced Research Institute
Sofia, Bulgaria
t.georgieva@rndc.bg

Ivo Radulov

Rakovski National Defence College
Defense Advanced Research Institute
Sofia, Bulgaria
i.radulov@rndc.bg

Abstract— A two-layered analytical approach was applied to assess the influence of actual experience with the state and functioning of procedural justice, trust in leadership, and the level of digitalization of equipment in military formations in a peacetime context on service members' expectations regarding the performance of strategic, operational, and tactical levels of leadership in the command and control (C2) system during a hypothetical operational scenario. The adopted methodological framework allows for a parallel analysis of the substantive relationships among the included variables while simultaneously accounting for the mental transition between cognitive representations of actual experience and those constructed at the level of abstract hypothesizing.

In conditions of compressed timeframes and escalating complexity, dynamism, and multi-layered operational environments, modern C2 system are conceptualized around the principle of centralized command and decentralized execution, which functions as a system-forming mechanism for maintaining operational tempo and ensuring coordination coherence across different levels of command.

Procedural justice in peacetime and established trust in leadership are recognized as fundamental prerequisites for effective mission command, as they foster perceptions of legitimacy, commitment, and willingness to take initiative at lower levels of command.

Digitalization, including the development of artificial intelligence transforms command into the so-called “digital mission command” [1, p.162] emphasizing the achievement of decision superiority. This requires leaders at all levels to interpret and effectively act upon digitally provided information, thereby enabling closer and faster alignment between strategic objectives and tactical actions on the battlefield.

The empirical study was conducted on a representative sample of 1,257 service members and included analysis of

data collected through a battery of questionnaires covering psychological and organizational measures.

Correlation and mediation analyses demonstrate that procedural justice, trust in leadership, and digitalization exert systematic and multi-level effects on expectations of leadership effectiveness in C2 systems in the context of real operational scenario. The results indicate that digitalization and trust in leadership enhance command effectiveness through the mediating role of procedural justice, with digitalization exhibiting a stronger mediating effect than trust.

Keywords— procedural justice, C2 leadership, digitalization, trust in leader.

I. INTRODUCTION

The contemporary security environment is characterized by a high degree of dynamism, complexity, and uncertainty, thereby placing increasing demands on the effectiveness of Command and Control (C2) systems. Within this context, the principle of centralized command and decentralized execution has become a system-defining mechanism for ensuring operational coherence and sustaining the tempo of operations in multi-layered operational environments [2], [3], particularly in situations characterized by “unclear situational awareness, high dynamics, a high degree of uncertainty in evolving processes, and the presence of well-prepared response forces” [4, p. 49]. The practical realization of the benefits associated with effective management has generated sustained scholarly interest in governance methods and instruments [5, p. 9]. Under conditions of high uncertainty, command effectiveness is determined not only by formal structures but also by the capacity for adaptive allocation

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.123>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

of authority and responsibilities across different levels of command [6].

Within the field of organizational psychology, it is well established that perceived leadership effectiveness is shaped by a constellation of interrelated factors, among which procedural justice plays a central role. Procedural justice refers to the perceived objectivity, consistency, and transparency of organizational procedures [7], [8]. Empirical research consistently shows that higher levels of procedural justice are associated with increased leadership legitimacy, stronger organizational commitment, and a greater propensity for proactive behavior [7], [8], [9], [10], [11]. In military organizations, these effects are further amplified by the need for decision-making under conditions of risk and time pressure, where clearly defined procedural frameworks reduce uncertainty and facilitate coordination [12].

Trust in leadership is regarded as a second key determinant of organizational effectiveness. In theoretical models of transformational leadership, trust is defined as a primary mechanism through which leaders influence the attitudes and behaviors of subordinates [13], [14]. Furthermore, Kramer (1999) conceptualizes trust as a mediating variable linking organizational practices to behavioral outcomes, thereby functioning as an intervening mechanism within complex social systems [15].

Alongside these organizational determinants, digitalization has emerged as a structurally defining factor in the transformation of C2 systems [16, 17]. The advancement of information and communication technologies, including artificial intelligence, has led to the development of the concept of “digital mission command”, aimed at achieving information superiority and decision advantage [1, p.162]. From the perspective of network society theory, it has been emphasized that digital technologies reconfigure structures of power and coordination, thereby enabling increased integration and adaptability [18]. In the context of military systems, it has been argued that command effectiveness depends on the extent to which information flows and technological solutions are integrated into decision-making processes [19]. The inclusion of diverse stakeholders in these debates can ensure that safety and ethical concerns are addressed without impeding progress [20, p. 17]. In this regard, “good governance is based on decisions made on the basis of thorough analyses and choices grounded in in-depth research.” [21, p.159, 160].

Despite the substantial body of theoretical and empirical research, the question of the combined effects of procedural justice, trust in leadership, and digitalization on perceptions of leadership effectiveness within hypothetical operational scenarios and reactive management through the implementation of the “Lessons Learned” process [22, p. 455] remains insufficiently explored. This issue is particularly salient in light of the cognitive limitations inherent in human evaluative processes. It has been argued that under hypothetical conditions, individuals rely on heuristic strategies and simplified mental models, which

may result in reduced differentiation between conceptually proximate categories [23]. Similarly, the theory of bounded rationality suggests that individuals tend to settle for “satisficing” decisions based on simplified cognitive schemas rather than pursuing optimal evaluations [24].

Within organizational systems, such cognitive mechanisms may give rise to holistic and weakly differentiated perceptions of leadership effectiveness across different levels. This perspective is consistent with the systems approach to organizations, which posits that organizational phenomena should be understood as the outcome of interactions among interdependent elements rather than as isolated cause-and-effect relationships [25].

The present study is situated within this integrative theoretical framework. Employing a two-layer analytical design, it investigates how military personnel’s real-world organizational experiences related to procedural justice, trust in leadership, and the level of digitalization shape their expectations regarding leadership effectiveness at the strategic, operational, and tactical levels within a hypothetical operational scenario. The methodological approach enables both the simultaneous modeling of empirical relationships among the examined variables and the analysis of the cognitive transition from experienced organizational contexts to abstract evaluative constructs.

As a result, the study advances the theoretical understanding of the multifactorial determinants of C2 leadership effectiveness by integrating organizational, psychological, and technological dimensions within a unified analytical framework. At the same time, it offers a more robust basis for interpreting empirical findings in light of the cognitive limitations inherent in evaluations grounded in hypothetical scenarios, thereby enhancing both their validity and practical applicability.

II. MATERIALS AND METHODS

A. Sample

The study sample comprises 1,257 military personnel, representing a refined subset of the initial pool of respondents (1,600 individuals). The selection was carried out by excluding respondents who provided identical ratings across all items of a questionnaire assessing military personnel’s perceptions of C2 leadership performance under conditions of potential real combat operations. This approach was adopted in order to enhance the reliability and validity of the data, ensuring that only participants who provided meaningful and differentiated responses were included in the analysis.

The sample was described according to the following parameters: gender, age, rank, and participation in overseas missions. The gender distribution is 79% male and 21% female, reflecting the traditional structure of the armed forces.

The age distribution indicates that the largest proportion of respondents falls within the 41–50 age group (39%), followed by those aged 31–40 (30%). Younger respondents (21–30 years) account for 22%, while those aged 51–60

represent 8%, and 1% are under the age of 20. These demographic data suggest that the sample is dominated by military personnel in active and mature age groups with accumulated professional experience.

In terms of rank, the percentage distribution is as follows: senior officers (41%), junior officers (36%), non-commissioned officers (15%), enlisted personnel (6%), and officer candidates (2%). This distribution demonstrates a clear predominance of the officer corps within the sample, which should be taken into account when interpreting the results, as it reflects a stronger representation of managerial-level perspectives within the military organization.

The relatively high proportion of senior officers (41%) in the sample [26] may have significantly influenced subjective assessments of procedural justice and other included construct, as this group occupies managerial and command positions and is directly involved in decision-making, resource allocation, control, and the evaluation of subordinate personnel. This suggests that their perceptions of procedural fairness may differ from those of military personnel at lower hierarchical levels.

The majority of respondents (76%) have not participated in overseas missions. This finding suggests that the study predominantly reflects perceptions of military personnel without direct operational experience in international or combat missions.

B. Methods

The empirical study involves the analysis of data collected through a battery of questionnaires covering psychological and organizational dimensions [26, 27]. These instruments are designed to assess military personnel's perceptions of the effectiveness of strategic, operational, and tactical leadership within the C2 system under conditions of a real military operation. The analytical focus is placed on the relationships between these perceptions and evaluations of the levels of procedural justice, trust in leadership, and the degree of digitalization in the peacetime functioning of military units, also measured through the questionnaires included in the battery. The data were processed using statistical methods (factor analysis, correlation analysis, regression models, etc.).

TABLE I. DESCRIPTIVE STATISTICS AND INTERNAL CONSISTENCY

Descriptive Statistics	Descriptive Statistics and Internal Consistency					
	Variable	Number of Items	Cronbach's Alpha	Mean	SD	Mean / № of Items
Independent variables	1. Procedural Justice	7	0.858	22.66	5.18	3.24
	2. Digitalization	2	0.670	5.65	2.10	2.84
	3. Trust in the Leader	12	0.929	48.39	8.65	4.02
Dependent variables	4.C2 Leadership	3	0.910	9.17	2.70	3.06
	5. Strategic Command	1	–	3.00	0.975	3.00
	6. Operational Command	1	–	3.03	0.988	3.03
	7. Tactical Command	1	–	3.14	0.976	3.14

C. Research design of the empirical study

1) Research Objective

To examine the impact of procedural justice, trust in leadership, and digitalization on military personnel's perceptions of the effectiveness of C2 leadership (tactical, operational, strategic, and overall) in real combat operations.

2) Research Tasks

a) To investigate the *influence* of procedural justice, trust in leadership, and the level of digitalization in a peacetime context on military personnel's perceptions of the effectiveness of C2 leadership in real combat operations.

b) To analyze *differences* in military personnel's perceptions of the effectiveness of the three levels of C2 leadership (tactical, operational, and strategic) in real combat operations.

3) Hypotheses

a) H1. Procedural justice, trust in leadership, and the level of digitalization in a peacetime context exert a positive (directly proportional) effect on military personnel's perceptions of the effectiveness of C2 leadership in real combat operations.

b) H2. Trust in leadership and the level of digitalization mediate the relationship between procedural justice and military personnel's perceptions of the effectiveness of C2 leadership in real combat operations.

c) H3. Trust in leadership is more strongly associated with perceptions of effectiveness at the tactical level of leadership, whereas the level of digitalization and procedural justice are more strongly associated with effectiveness at the operational and strategic levels within the C2 system.

The hypotheses are based on the described research [9], [10], [11], [13], [14], [15].

III. RESULTS

A. Descriptive Statistics

The descriptive statistics are presented in „Tab. I“. The reported descriptive statistics allow for a comprehensive analysis of central tendencies and the reliability of the scales employed.

The leading variable in terms of mean value (Mean/number of items) is trust in leadership ($M = 4.03$), indicating a high level of trust in managerial governance. This result suggests that leadership is perceived as a stable and positive factor within the organizational context.

The mean value of procedural justice ($M = 3.24$) reflects a moderately positive perception of fairness in the functioning of normative and administrative processes within the organization. The lowest mean value is observed for digitalization ($M = 2.83$), which is associated with deficiencies in the technological environment and the implementation of digital solutions.

The coefficients of internal consistency (Cronbach's alpha) are acceptable. Trust in leadership ($\alpha = 0.929$), C2 leadership ($\alpha = 0.910$), and procedural justice ($\alpha = 0.858$) demonstrate excellent reliability, indicating that the items within these scales consistently measure the respective constructs. Digitalization does not reach the conventional threshold for reliability but may be considered acceptable as a compromise ($\alpha = 0.670$).

In summary, the results outline a clear pattern of high trust in leadership, combined with moderate evaluations of organizational processes and lower evaluations of digitalization. The reliability of most scales is high, providing a solid empirical and methodological foundation for the conclusions drawn. Digitalization emerges as a problematic aspect, standing out as a potential area for organizational development and improvement. This finding is consistent with previous research by Grozdanova, which identifies the deteriorating condition of

armament and equipment, clothing, and gear as key factors contributing to the decline in the status of military personnel [27]. The tactical level of C2 leadership demonstrates significant differences, albeit with small effect sizes compared to the other two levels, which calls for a more in-depth analysis of the influencing factors.

A. Correlation Analyses

Correlation and mediation analyses were conducted, demonstrating that procedural justice, trust in leadership, and digitalization exert a systematic and multi-level influence on military personnel's perceptions of C2 leadership effectiveness in the context of real military situations. The correlation analyses of the variables included in the study are presented in "Tab. II".

The results indicate that all examined variables are positively and statistically significantly correlated. Procedural justice shows the strongest moderate associations with trust in leadership ($r = 0.45$, $p < 0.01$) and with digitalization ($r = 0.43$, $p < 0.01$). Significant moderate relationships are also observed with the different levels of C2 leadership ($r = 0.34$ – 0.40 , $p < 0.01$). This correlation pattern highlights the central role of procedural justice as a key organizational factor.

Digitalization exhibits low but significant correlations with all variables except itself, including trust in leadership ($r = .19$, $p < 0.01$) and the leadership dimensions ($r = 0.24$ – 0.29 , $p < 0.01$), suggesting a more indirect influence on organizational processes. Trust in leadership is weakly to moderately associated with all levels of leadership ($r = 0.27$ – 0.30 , $p < 0.01$), indicating its consistent role across different managerial contexts.

In summary, the results emphasize the importance of procedural justice as a leading factor associated both with trust and leadership effectiveness. Digitalization emerges as a component with a more limited yet consistent influence.

TABLE II. PEARSON CORRELATION ANALYSIS

Pearson Correlation Analysis Variables	Correlation Coefficients					
	Digitalization	Trust in the leader	C2 Leadership	Strategic Command	Operational Command	Tactical Command
1. Procedural justice	0.43**	0.45**	0.40**	0.37**	0.39**	0.34**
2. Digitalization	—	0.19**	0.29**	0.28**	0.29**	0.24**
3. Trust in the leader	—	—	0.30**	0.27**	0.27**	0.30**

TABLE III. MULTIPLE REGRESSION PREDICTING C2 LEADERSHIP

Predictor	Multiple regression coefficients				
	B	SE B	β	t	p
Constant	2.663	0.443	—	6.01	< 0.001
1. Procedural justice	0.135	0.017	0.26	7.96	< 0.001
2. Trust in the leader	0.049	0.009	0.16	5.22	< 0.001

Predictor	Multiple regression coefficients				
	<i>B</i>	<i>SE B</i>	β	<i>t</i>	<i>p</i>
3. Digitalization	0.190	0.038	0.15	5.01	< 0.001

Note. $N = 1122$. $R = 0.44$, $R^2 = 0.19$, Adjusted $R^2 = 0.19$, $F(3, 1118) = 88.64$, $p < 0.001$. Durbin-Watson = 1.96.

B. The influence of procedural justice, trust in leadership, and the level of digitalization in a peacetime context on military personnel's perceptions of the effectiveness of C2 leadership in real combat operations

The influence of procedural justice, trust in leadership, and the level of digitalization in a peacetime context on military personnel's perceptions of the effectiveness of C2 leadership in real combat operations was assessed using regression models.

A multiple regression analysis was conducted "Tab. III" to examine the extent to which procedural justice, trust in leadership, and digitalization predict C2 effectiveness in a potential combat situation. The model is statistically significant, $F(3, 1118) = 88.64$, $p < 0.001$, and explains 19% of the variance in C2 leadership effectiveness ($R^2 = 0.19$). All predictors are significant: procedural justice ($\beta = 0.26$, $p < .001$), trust in leadership ($\beta = 0.16$, $p < .001$), and the level of digitalization ($\beta = 0.15$, $p < 0.001$). The results indicate that higher values of these variables are associated with higher levels of perceived C2 leadership effectiveness.

In order to build and further detail the overall empirical picture, an additional stepwise multiple regression analysis was conducted "Tab. IV".

The results presented in the table indicate that in Model 1, procedural justice is a significant predictor and explains 15.5% of the variance. In Model 2, the variable trust in leadership was added, which is associated with a small but statistically significant increase in explained variance ($\Delta R^2 = 0.02$, $p < 0.001$). In Model 3, the level of digitalization further improves the model ($\Delta R^2 = 0.02$, $p < 0.001$). The final model explains 19.2% of the variance in C2 leadership effectiveness, $F(3, 1118) = 88.64$, $p < 0.001$. Overall, the results indicate that procedural justice is the key factor, while trust and digitalization have a complementary effect. Trust in leadership and digitalization contribute a small but statistically significant incremental effect. The findings suggest that rather than dominant effects, cumulative effects are observed.

The obtained results support Hypothesis 1, namely that procedural justice, trust in leadership, and the level of digitalization in a peacetime context exert a positive (directly proportional) influence on military personnel's perceptions of the effectiveness of C2 leadership in real combat operations.

Hypothesis 2, according to which trust in leadership and the level of digitalization mediate the relationship between procedural justice and military personnel's perceptions of the effectiveness of C2 leadership in real combat

operations, is examined through the Baron & Kenny (1986) model [29], which postulates the application of three regression models to extract the effects: $X \rightarrow M$, $X \rightarrow Y$, and $M \rightarrow Y$, where the effect in the second equation must be greater than that established in the third equation. This final condition was satisfied only in the model in which procedural justice serves as the predictor (X), and trust in leadership and the level of digitalization function as mediators (M). In "Tab. V" are presented the independent and joint mediating effects of the two variables on C2 leadership effectiveness in a potential combat situation (Y).

The results of the mediation analyses indicate a consistent and statistically significant indirect effect of procedural justice on perceptions of C2 leadership effectiveness in a real combat situation through two mediators—trust in leadership and digitalization.

In Model 1, procedural justice has a strong effect on trust in leadership ($B = 0.749$, $p < 0.001$), which in turn significantly predicts perceptions of C2 leadership effectiveness in a real combat situation ($B = 0.049$, $p < 0.001$). The indirect effect is small but statistically significant ($a \times b = 0.037$, 95% CI [0.020; 0.059]), accounting for approximately 17.9% of the total effect. The presence of a significant direct effect ($B = 0.170$, $p < 0.001$) indicates partial mediation.

In Model 2, procedural justice also significantly predicts digitalization ($B = 0.176$, $p < 0.001$), which in turn has a stronger effect on the dependent variable ($B = 0.188$, $p < 0.001$). The indirect effect (0.033, 95% CI [0.018; 0.054]) is comparable in magnitude to that in Model 1 and accounts for approximately 15.9% of the total effect, again indicating partial mediation.

The full model, which includes both mediators simultaneously, shows a larger total indirect effect (0.070, 95% CI [0.040; 0.100]), explaining approximately 33.8% of the relationship between procedural justice and perceptions of C2 leadership effectiveness in a real combat situation. This result indicates a cumulative mediating effect, where the two mechanisms operate in a complementary manner. Despite this, the direct effect remains significant, confirming partial mediation.

Overall, the results partially support Hypothesis 2, namely that procedural justice influences perceptions of C2 leadership effectiveness in a real combat situation both directly and indirectly through increased trust in leadership and perceived level of digitalization, with both mediators contributing similarly to the explanation of the effect.

C. Differences in military personnel's perceptions of the effectiveness of the three levels of C2 leadership (tactical, operational, and strategic) in real combat operations

The empirical evidence testing the third formulated hypothesis is presented in "Tab. VI". The assumption summarizes that trust in leadership is more strongly associated with perceptions of the effectiveness of tactical-level leadership in a real combat situation, whereas the level of digitalization and procedural justice are more strongly associated with perceptions of the effectiveness of operational and strategic-level leadership.

The analysis of the results indicates that the empirical findings do not provide conclusive statistical support for the third hypothesis, but rather partially support it at a descriptive level. The correlation coefficients demonstrate

values in the predicted direction: trust in leadership shows the highest association with perceptions of tactical-level C2 leadership effectiveness ($r = 0.30$), which is consistent with the hypothesis. The relationships of digitalization ($r = 0.29$) and procedural justice ($r = 0.39$) show slightly higher values at the operational and strategic levels, which also aligns with the theoretical assumption.

At the same time, the results of the Fisher r-to-z analysis show that all comparisons between levels are $p > 0.05$, indicating that the differences between correlations are not statistically significant. The conclusion is that the observed differences between command levels are too small to claim that a given factor is a significantly stronger predictor for one level compared to another.

TABLE IV. STEPWISE MULTIPLE REGRESSION PREDICTING C2 LEADERSHIP

Predictor	Multiple regression coefficients								
	Model 1 B (SE)	Model 2 B (SE)	Model 3 B (SE)	R	R ²	ΔR^2	F	df	p
Constant	4.512 (0.333)***	2.987 (0.443)***	2.663 (0.443)***	—	—	—	—	—	—
1. Procedural justice	0.205 (0.014)***	0.169 (0.016)***	0.135 (0.017)***	0.39	0.16	0.16	204.71	(1, 1120)	< 0.001
2. Trust in the leader	—	0.048 (0.009)***	0.049 (0.009)***	0.42	0.17	0.02	117.87	(2, 1119)	< 0.001
3. Digitalization	—	—	0.190 (0.038)***	0.44	0.19	0.02	88.64	(3, 1118)	< 0.001

Note. $N = 1122$. $\Delta R^2 = \text{change in } R^2$. *** $p < 0.001$.

In conclusion, Hypothesis 3 receives partial support at a descriptive level (the trends are in the expected direction), but is not statistically confirmed, as no significant differences between correlations are found. It is reasonable

to conclude that, in military personnel's perceptions, the examined predictors do not demonstrate statistically significant differentiation in relation to the effectiveness of the three command levels in real combat situations.

TABLE V. MEDIATION MODELS

Mediation Models	Mediation Analysis Coefficients									
	Independent Variable (X)	Mediator (M)	Dependent Variable (Y)	$X \rightarrow M$ (B, SE, p)	$M \rightarrow Y$ (B, SE, p)	$X \rightarrow Y$ Direct Effect (B, SE, p)	Indirect Effect (a×b)	95% CI (Bootstrap)	Total Effect (c)	% Mediation
Model 1	Procedural justice	Trust in the leader	Expectations of leadership in the C2 system	B = 0.749, SE = 0.048, p < 0.001	B = 0.049, SE = 0.011, p < 0.001	B = 0.170, SE = 0.017, p < 0.001	0.037	~[0.020; 0.059]*	B = 0.207, SE = 0.015, p < 0.001	~17.9%
Model 2	Procedural justice	Digitalization	Expectations of leadership in the C2 system	B = 0.176, SE = 0.011, p < 0.001	B = 0.188, SE = 0.043, p < 0.001	B = 0.170, SE = 0.017, p < 0.001	0.033	~[0.018; 0.054]*	B = 0.207, SE = 0.015, p < 0.001	~15.9%
Complex Model	Procedural justice	Trust in the leader Digitalization	Expectations of leadership in the C2 system	Overall indirect effect	—	—	0.070	~[0.040; 0.100]*	B = 0.207, SE = 0.015, p < 0.001	~33.8%

TABLE VI. CORRELATION COEFFICIENTS AND FISHER R-TO-Z ANALYSIS

Predictor	Correlation Coefficients and Fisher r-to-z Analysis						
	<i>Strategic Command</i> r	<i>Operational Command</i> r	<i>Tactical Command</i> r	Strongest association	Fisher r-to-z (key comparisons)	Significance of differences	Conclusion
1. Procedural justice	0.37**	0.39**	0.34**	<i>Strategic Command</i>	$z \approx 0.58-1.45$	$p > 0.05$	No significant differences between levels
2. Digitalization	0.28**	0.29**	0.24**	<i>Operational Command</i>	$z \approx 1.15-1.45$	$p > 0.05$	No significant differences between levels
3. Trust in the leader	0.27**	0.27**	0.30**	<i>Tactical Command</i>	$z \approx 0.98$	$p > 0.05$	Descriptive but not statistically significant trend

IV. DISCUSSION

The interpretation of the obtained results should be considered in the context of the nature of the measured data. The present study is based on military personnel's perceptions of a hypothetical or projected combat situation rather than actual operational conditions; therefore, the obtained assessments reflect cognitive and perceptual models rather than behavioral responses in a real environment. This circumstance represents a significant methodological factor, as human judgments under conditions of hypotheticality are formed through cognitive heuristics and simplified mental models, which may reduce sensitivity to subtle differences between alternative scenarios [23]. In such conditions, individuals tend to generalize their evaluations and attribute similar significance to different but conceptually close categories. Under bounded rationality individuals do not process the full amount of available information but rely on simplified cognitive schemas, which may lead to a potential "smoothing" of differences between strategic, operational, and tactical perceptions, especially when assessments are made without real operational experience in the specific context [24].

The present study provides empirical evidence for the complex nature of the factors shaping perceptions of C2 leadership effectiveness in conditions approximating real combat situations. The obtained results confirm that organizational and technological determinants do not operate in isolation but form an interconnected system of influences, which is consistent with the systems approach to leadership [30]. The central role of procedural justice in the models aligns with established theoretical assumptions in organizational psychology. Perceived justice is identified as a key factor in building trust and leadership legitimacy [7], [31]. The results of the present study support these assumptions, showing that procedural justice has the strongest relationship with perceptions of C2 leadership effectiveness in a real combat situation. In the context of military organizations, this is particularly important, as clear and consistent procedures reduce uncertainty and support decision-making under conditions of risk [12].

The role of trust in leadership as a mediator confirms classical leadership models that regard trust as a core mechanism of effectiveness. Trust is identified as a core

element of transformational leadership and a key factor for engagement and effectiveness [13], [14]. The present results indicate that although the direct effect of trust is more moderate, its mediating role is substantial, which corresponds to the understanding of trust as a "switching mechanism" between organizational practices and behavioral outcomes [15].

Digitalization also demonstrates a significant, albeit more moderate, role, which is consistent with contemporary concepts of digital and networked governance. It is stated that information technologies transform organizational structures and processes by creating conditions for higher coordination and efficiency [18]. In addition, it is emphasized that the effectiveness of C2 systems depends on the ability to integrate information and technology into the decision-making process [19]. The present study confirms this logic by showing that digitalization has an indirect effect through the improvement of organizational processes.

A particularly important contribution of the study is the identification of a cumulative mediating effect. It is argued that multiple mediation models can operate simultaneously and mutually reinforce each other's effects, as proposed in [29]. The results indicate that trust and digitalization function as complementary mechanisms, supporting the idea of synergy between human and technological factors.

Regarding the differences between the levels of C2 leadership, the results show statistically significant but weak effects. The higher evaluations of the tactical level can be interpreted through its immediate proximity to real actions and the greater visibility of leadership behavior. This is consistent with the concept of "proximal leadership," according to which perceptions of leadership are stronger at lower hierarchical levels. The absence of substantial differences between the strategic and operational levels suggests that military personnel's perceptions are formed in a similar way at higher levels, where the distance from execution is greater [32].

It is emphasized that, from the perspective of decision-making theory under uncertainty, real differences in cognitive evaluations across management levels become most pronounced under conditions of actual stress, time pressure, and high responsibility. In the absence of such conditions (as is the case in projected scenarios),

differentiation between levels of perception is often reduced.

In this context, the lack of statistically significant differences between correlation coefficients may be interpreted not as an absence of theoretical differentiation, but as a result of contextual “smoothing” of perceptions. Military personnel are likely to perceive procedural justice, trust, and digitalization as general systemic factors influencing all levels of C2 leadership in a similar manner, without clearly distinguishing between them in a hypothetical situation.

This observation is consistent with the systems approach to organizations, according to which cognitive evaluations in complex systems are often formed as holistic representations rather than strictly differentiated structures [12]. In this sense, perceived effectiveness of different levels of C2 leadership may be understood as part of a unified mental schema rather than as separate and independently evaluated constructs.

V. CONCLUSIONS

In conclusion, the results of the study confirm that C2 leadership effectiveness is shaped by a complex interaction between procedural justice, trust in leadership, and the level of digitalization. The effects are cumulative rather than competitive. In line with theoretical models of organizational justice, transformational leadership, and the network society, the study demonstrates that sustainable leadership in contemporary military systems requires the integration of human and technological factors within a fair and trust-based organizational environment [33]. From a practical perspective, the results point to the need for the simultaneous development of organizational justice, trust, and the digital environment as interrelated elements for enhancing the effectiveness of C2 leadership.

ACKNOWLEDGMENT

The document was developed under the National Scientific Programme “Security and Defence”, funded by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 Oct. 2021.

REFERENCES

- [1] A. T. Bollmann and T. Heltberg, “The Strategic Corporal, the Tactical General, and the Digital Coup d’oeil – Military Decision-Making and Organizational Competences in Future Military Operations,” *Scandinavian Journal of Military Studies*, vol. 6, no. 1, pp. 151–168, Aug. 2023.
- [2] NATO, *NATO Digital Transformation / Digital Mission Command Concepts*. Brussels, Belgium, 2020.
- [3] V. Vasileva and V. Aleksandrova, “Application of NATO models for building information infrastructure in crisis conditions,” in *Proceedings of the Romanian Military Thinking International Scientific Conference*, Bucharest, Romania, 2024, pp. 232–247.
- [4] D. Ginev, *National Crisis Management Capabilities – State and Prospects* [in Bulgarian]. Sofia, Bulgaria: Videlina, 2024.
- [5] P. Stoilov, *Administrative Management in Defense* [in Bulgarian]. Sofia, Bulgaria: DioMira, 2022.
- [6] M. van Creveld, *Command in War*. Cambridge, MA, USA: Harvard University Press, 1985.
- [7] J. Greenberg, “A taxonomy of organizational justice theories,” *Academy of Management Review*, vol. 12, no. 1, pp. 9–22, 1987.
- [8] T. R. Tyler, *Why People Obey the Law*. New Haven, CT, USA: Yale University Press, 1990.
- [9] D. De Cremer, R. van Dijke, and A. Bos, “Leader’s procedural justice affecting identification and trust,” *The Leadership Quarterly*, vol. 17, no. 6, pp. 602–617, 2006.
- [10] R. Cropanzano and M. S. Mitchell, “Social exchange theory: An interdisciplinary review,” *Journal of Management*, vol. 31, no. 6, pp. 874–900, 2005.
- [11] M. Klimchak, J. A. O’Neill, and B. S. Palmer, “Perceptions of organizational support, work–life balance, and employee well-being: The mediating role of work engagement,” *Journal of Organizational Psychology*, vol. 20, no. 2, pp. 36–50, 2020.
- [12] K. E. Weick, *Sensemaking in Organizations*. Thousand Oaks, CA, USA: Sage, 1995.
- [13] B. M. Bass, *Leadership and Performance Beyond Expectations*. New York, NY, USA: Free Press, 1985.
- [14] B. J. Avolio, *Full Leadership Development: Building the Vital Forces in Organizations*. Thousand Oaks, CA, USA: Sage, 1999.
- [15] R. M. Kramer, “Trust and distrust in organizations: Emerging perspectives, enduring questions,” *Annual Review of Psychology*, vol. 50, pp. 569–598, 1999.
- [16] V. Vasileva and V. Gagamova, “Application of simulation modeling in education and scientific research: An exploration through predictive scenarios of cybersecurity threats,” in *Proceedings of the 18th International Conference on Education, Research and Innovation (ICERI 2025)*, Seville, Spain, Nov. 10–12, 2025, pp. 8962–8969.
- [17] V. Aleksandrova, V. Tagareva, and V. Vasileva, “Regarding the needs for knowledge and artificial intelligence as a guarantee for the change of modern Bulgaria—ethical aspects of the application of artificial intelligence in autonomous systems,” in *Proceedings of the XVIII International Conference on Open and Underwater Mining of Minerals*, Varna, Bulgaria, 2025, pp. 225–234.
- [18] M. Castells, *The Rise of the Network Society*. Oxford, U.K.: Blackwell, 1996.
- [19] D. S. Alberts and R. E. Hayes, *Power to the Edge: Command and Control in the Information Age*. Washington, DC, USA: CCRP, 2003.
- [20] M. I. Nenovska, “Biosecurity concerns and benefits of artificial intelligence use in the life sciences,” in *Proceedings of the IX International Scientific Conference CONFSEC*, Borovets, Bulgaria, Dec. 8–11, 2025.
- [21] K. Peicheva, *Development of the Public Service “Defense” in Bulgaria* [in Bulgarian]. Sofia, Bulgaria: Academic Publishing House “Prof. Marin Drinov”, 2014.
- [22] Z. Zdravkov, Zh. Petrov, A. Atipova, and S. Stoykov, “Synchronization of sociological survey processes for the quality of education and the lessons-learned process at the Rakovski National Defence College, in *Proceedings of the International Scientific Conference “Defense Technologies”*, Shumen, Bulgaria, 2022, pp. 452–461, ISSN 2367-7902.
- [23] D. Kahneman, *Thinking, Fast and Slow*. New York, NY, USA: Farrar, Straus and Giroux, 2011.
- [24] H. A. Simon, *Models of Man: Social and Rational*. New York, NY, USA: Wiley, 1957.
- [25] V. Vasileva and J. Hlebarov, “Methodology for improving cyber awareness competencies of employees in public administration,” in *Proceedings of the International Conference on Application of Information and Communication Technology, Statistics and Economic Education (ICAICTSEE 2020)*, Sofia, Bulgaria, 2020, pp. 278–285, published by UNWE Publishing Complex, 2021.
- [26] *Report on the Results of a Representative Sociological Study on the Topic: “Motivation of Personnel in the Formations of the Armed Forces of the Republic of Bulgaria”*. Sofia, Bulgaria: Defence Advance Research Institute, Rakovski National Defence College, Nov. 2025, Reg. No. SI-29-10294/25.11.2025, unpublished.

- [27] V. Vasileva, V. Aleksandrova, and A. Guncheva, "Developing information technologies and digital transformation to answer modern educational and security challenges," in *Proceedings of the International Conference on Application of Information and Communication Technology, Statistics and Economic Education (ICAICTSEE 2017)*, Sofia, Bulgaria: UNWE Publishing Complex, 2017, pp. 300–305.
- [27] T. Grozdanova, *Social Status of Military Personnel in the Years of Transition* [in Bulgarian]. Sofia, Bulgaria: IK VIDJI, 2024.
- [29] R. M. Baron and D. A. Kenny, "The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations," *Journal of Personality and Social Psychology*, vol. 51, no. 6, pp. 1173–1182, 1986.
- [30] P. M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York, NY, USA: Doubleday, 1990.
- [31] T. R. Tyler and S. L. Blader, "The group engagement model: Procedural justice, social identity, and cooperative behavior," *Personality and Social Psychology Review*, vol. 7, no. 4, pp. 349–361, 2003.
- [32] G. Klein, *Sources of Power: How People Make Decisions*. Cambridge, MA, USA: MIT Press, 1998.
- [33] D. Tashkov, "Building organizational resilience: Strategic approaches," *Military Journal*, vol. 132, no. 1, pp. 5–13, Sofia, Bulgaria: Publishing House "G. S. Rakovski," 2025, ISSN 2534-8388.

Lightweight Comparative Evaluation of Quantum and Hybrid Quantum-Classical Machine Learning Models for Intrusion Detection

Genadiy Gospodinov

Computer Sciences
University of Library Studies and
Information Technologies
Sofia, Bulgaria
g.gospodinov@unibit.bg
ORCID: [0009-0007-0792-2162](https://orcid.org/0009-0007-0792-2162)

Tamara Ristovska

Computer Sciences
University of Library Studies and
Information Technologies
Sofia, Bulgaria
t.ristovska@unibit.bg
ORCID: [0009-0005-9870-1327](https://orcid.org/0009-0005-9870-1327)

Tito Titov

Computer Sciences
University of Library Studies and
Information Technologies
Sofia, Bulgaria
t.titov@unibit.bg

Kiril Nikolov

Computer Sciences
University of Library Studies and
Information Technologies
Sofia, Bulgaria
k.nikolov@unibit.bg

Andriyan Stoilov

Computer Sciences
University of Library Studies and
Information Technologies
Sofia, Bulgaria
a.stoilov@unibit.bg

Kliment Toshkov

Computer Sciences
University of Library Studies and
Information Technologies
Sofia, Bulgaria
k.toshkov@unibit.bg
ORCID: [0009-0000-7449-9455](https://orcid.org/0009-0000-7449-9455)

Abstract— Quantum machine learning (QML) has recently emerged as a promising research direction at the intersection of artificial intelligence, quantum computing, and cybersecurity. Among its potential applications, intrusion detection remains particularly relevant due to the growing complexity of cyber threats and the increasing need for adaptive and efficient detection mechanisms. This paper explores the applicability of lightweight quantum and hybrid quantum-classical machine learning approaches for intrusion detection in resource-constrained experimental settings. The study is designed as a comparative analysis of selected models, including variational and kernel-based quantum techniques, alongside a conventional classical baseline, in order to evaluate their practical potential for cybersecurity tasks. The experimental framework relies on a reduced and preprocessed cybersecurity dataset and is implemented in a simulated quantum environment using accessible open-source tools. The comparison considers standard performance indicators such as classification effectiveness and computational efficiency, while also reflecting on broader dimensions of model suitability for security-oriented applications. In addition to the technical evaluation, the paper addresses several ethical considerations associated with the use of QML in cybersecurity, including limited transparency, risks related to biased or imbalanced training data, and the operational implications of incorrect classifications in intrusion detection scenarios.

Rather than claiming immediate quantum advantage, the study aims to provide a realistic and methodologically grounded perspective on the current role of QML in cybersecurity research. The expected contribution is twofold - first, to outline a feasible experimental approach for evaluating QML methods in intrusion detection and second, to highlight the importance of combining performance-oriented assessment with ethical and interpretability-related considerations when examining emerging intelligent security solutions.

Keywords – Cybersecurity, hybrid quantum-classical models, intrusion detection, quantum machine learning

I. INTRODUCTION

The increasing complexity of contemporary cyber threats has intensified the need for adaptive, data-driven, and computationally efficient intrusion detection mechanisms. Intrusion Detection Systems (IDS) remain a central component of cybersecurity architectures because they support the identification of suspicious, anomalous or malicious activities within networked environments. Traditional rule-based IDS approaches are often limited by their dependence on predefined signatures and their reduced ability to detect previously unseen attacks. For this reason, machine learning has become a widely investigated direction in intrusion detection research, offering the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.207>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

possibility to learn patterns from traffic data and to distinguish between normal and malicious behavior under different operational conditions. [1] At the same time, the use of machine learning in network intrusion detection is not straightforward, since real network environments are dynamic, imbalanced, noisy, and difficult to represent through stable training data. [2]

A significant body of research has explored the application of classical machine learning methods such as support vector machines, decision trees, random forests, logistic regression, and neural networks for intrusion detection. These methods have shown promising results on benchmark datasets, especially when combined with appropriate preprocessing, feature selection, and class-balancing strategies. Public datasets such as NSL-KDD intrusion detection dataset, derived as an improved benchmark based on the Knowledge Discovery and Data Mining Cup 1999 (KDD'99) dataset, and the University of New South Wales Network Benchmark 2015 (UNSW-NB15) dataset have played an important role in enabling comparative IDS research, although they also have well-known limitations related to representativeness, redundancy, imbalance, and the gap between benchmark traffic and real operational environments. [3], [4] Therefore, IDS evaluation should not rely exclusively on high aggregate accuracy, but should also consider false positives, false negatives, feature reduction, computational cost, and the practical interpretability of the resulting model.

In parallel with the development of classical machine learning for cybersecurity, quantum computing has introduced new possibilities for computational modelling, optimization, and pattern recognition. Quantum machine learning (QML) has emerged as an interdisciplinary research field that investigates how quantum information processing can be used to enhance or reformulate machine learning tasks. [5] In particular, quantum kernel methods and variational quantum algorithms have attracted attention because they are compatible with the current stage of noisy intermediate-scale quantum technologies and can be implemented in simulated or cloud-based quantum environments. [6], [7] Quantum kernel approaches are based on the idea of embedding classical data into a quantum feature space, while variational quantum classifiers use parameterized quantum circuits trained through a classical optimization loop. [8], [9]

Despite this growing interest, the practical role of QML in cybersecurity remains exploratory. Current quantum hardware is still constrained by noise, limited qubit counts, circuit depth restrictions, and execution costs. As a result, many QML experiments are performed in simulated environments and rely on reduced datasets, a small number of features, and binary classification settings. These restrictions do not invalidate QML research, but they require careful methodological framing. In intrusion detection, where datasets may contain high-dimensional, imbalanced, and heterogeneous network traffic records, lightweight QML evaluation is particularly relevant because it allows researchers to test whether quantum and

hybrid quantum-classical models can be meaningfully compared with conventional machine learning baselines under realistic resource constraints.

This paper addresses this research context by presenting a lightweight comparative evaluation of selected quantum and hybrid quantum-classical machine learning models for intrusion detection. The study is not designed to claim immediate quantum advantage over established classical methods. Instead, it aims to provide a realistic and reproducible experimental perspective on how QML models can be implemented, evaluated, and interpreted in a constrained cybersecurity scenario. The proposed experimental design compares a conventional classical baseline with quantum and hybrid approaches, such as quantum kernel-based classification and variational quantum classification. The comparison focuses not only on classification effectiveness, but also on computational efficiency and broader suitability for security-oriented applications.

The motivation for this approach is twofold. First, intrusion detection represents a meaningful cybersecurity use case for testing emerging machine learning paradigms because it requires the identification of complex patterns in network data. Second, QML methods are still at an early stage of practical adoption, which makes small-scale, reproducible, and critically interpreted experiments more valuable than overly ambitious claims about quantum superiority. In this context, a lightweight experimental setting provides a balanced way to examine both the potential and the limitations of QML for intrusion detection. It also allows the research to remain technically feasible using open-source tools such as Python, scikit-learn, and Qiskit within a controlled virtualized environment. [10], [11], [12]

Another important aspect of this study is the inclusion of ethical and interpretability-related considerations. In cybersecurity, incorrect classifications may have operational consequences – false negatives can allow attacks to remain undetected, while false positives may overload analysts and reduce trust in the system. These concerns are especially relevant for models whose internal decision logic is difficult to interpret. Although QML models may offer new representational possibilities, their practical adoption in security contexts requires attention to transparency, reliability, bias in training data, and the responsible use of automated decision-support systems. This perspective is consistent with broader AI risk management principles, which emphasize trustworthy, accountable, and context-aware deployment of AI systems. [13]

The main contribution of this paper is a methodologically grounded and lightweight comparative framework for evaluating quantum and hybrid quantum-classical machine learning models in an intrusion detection scenario. The authors' specific contribution consists in designing and implementing a reproducible experimental workflow that adapts selected QML models to a reduced and preprocessed NSL-KDD dataset, compares them with a classical SVM baseline under the same experimental

conditions, and evaluates the obtained results through classification metrics, execution time, error distribution, and repeated-run stability. From an applied perspective, the obtained results can be used as a reference for researchers and security practitioners who need to assess the practical suitability of QML-based IDS models before extending the analysis to larger datasets, multiclass attack detection, noise-aware simulation, or real quantum backends. By doing so, the study positions QML not as a replacement for classical intrusion detection methods, but as an emerging research direction whose practical value must be assessed through careful, transparent, and reproducible experimentation.

The remainder of the paper is structured as follows. The Materials and Methods section describes the dataset preparation, preprocessing procedure, experimental environment, selected models, and evaluation metrics. The Results and Discussion section presents the comparative results, including classification performance, computational efficiency, and interpretation of the observed model behavior. Finally, the Conclusion summarizes the main findings, outlines the limitations of the study, and identifies possible directions for future research, including larger datasets, multiclass intrusion detection, noise-aware quantum simulation, and evaluation on real quantum backends.

II. MATERIALS AND METHODS

The methodology follows a simple but structured workflow – dataset selection, preprocessing and feature reduction, model implementation, evaluation, and visual comparison of the obtained results. A classical machine learning model is used as a baseline, while two QML-oriented approaches are included to represent kernel-based and variational quantum learning. This makes it possible to compare not only predictive performance, but also the practical behavior of the models in terms of execution time, stability, and suitability for intrusion detection scenarios. The experimental implementation relies on open-source tools, including Python, scikit-learn, Qiskit, and Qiskit Machine Learning, which supports the reproducibility of the study and keeps the technical setup accessible for further validation. Qiskit provides open-source tools for developing and executing quantum programs, while Qiskit Machine Learning includes building blocks such as quantum kernels and quantum neural networks for classification and regression tasks. [11]

A. Experimental Design and Dataset

The experiment was designed as a binary classification task for intrusion detection. Network traffic records were grouped into two main classes: normal traffic and attack traffic. This binary formulation was selected to keep the experiment computationally feasible while still preserving the central logic of intrusion detection, namely the distinction between legitimate and potentially malicious behaviour. Although multiclass intrusion detection can provide a more detailed view of attack categories, it would also increase the complexity of the experimental setting and require a larger feature space, which is less suitable for a lightweight QML evaluation.

For the purposes of the study, the NSL-KDD dataset was selected as the experimental data source. NSL-KDD is widely used in intrusion detection research and was introduced as an improved version of the original KDD'99 dataset, addressing some of its known redundancy-related issues. At the same time, it should not be treated as a perfect representation of real contemporary network traffic. The Canadian Institute for Cybersecurity explicitly notes that, although NSL-KDD remains useful as a benchmark for comparing intrusion detection methods, it still has limitations and does not fully reflect modern operational networks. This makes it appropriate for a controlled comparative experiment, but not for making broad deployment claims.

In this study, the dataset is used in a reduced form. The reduction is not only a practical decision, but also a methodological requirement. Quantum and hybrid quantum-classical models executed in simulated environments are sensitive to the number of input features and training samples. Therefore, a smaller and balanced subset of records is used to allow fair execution of all selected models under the same experimental conditions. The aim is not to maximize dataset scale, but to establish a reproducible comparison between a classical baseline, a quantum kernel-based model, and a variational quantum classifier.

B. Data Preprocessing and Feature Reduction

Before model training, the dataset undergoes several preprocessing steps. First, categorical attributes are transformed into numerical form, since the selected machine learning models require numerical input. The class labels are also converted into a binary representation, where normal records are assigned to one class and attack records to the other. After that, the data are scaled to avoid disproportionate influence from features with larger numeric ranges. This step is especially important for distance-based and kernel-based models, including support vector machines and quantum kernel classifiers.

A train-test split is then applied to separate the data used for model training from the data used for evaluation. The same split is preserved across all compared models in order to ensure that the results are directly comparable. Because the study focuses on lightweight QML experimentation, the dimensionality of the feature space is reduced before the models are trained. In the proposed setup, Principal Component Analysis (PCA) is used to reduce the input space to four numerical components. This number is small enough to be compatible with a simulated quantum circuit and, at the same time, sufficient to preserve a compact representation of the original traffic patterns.

The choice of four features is also linked to the quantum model design. In many QML implementations, the number of input features is closely related to the number of qubits or to the complexity of the feature map. A high-dimensional input space would make the experiment unnecessarily heavy and could obscure the comparative purpose of the study. For this reason, feature reduction is treated not as a loss of methodological depth, but as a

necessary step for aligning the cybersecurity dataset with the practical constraints of quantum simulation.

C. Compared Models and Experimental Environment

Three models are included in the comparative evaluation. The first model is a classical Support Vector Machine, used as a baseline. SVMs are suitable for this role because they are established supervised learning methods for classification and are commonly used in benchmark classification tasks. The scikit-learn documentation describes support vector machines as supervised methods applicable to classification, regression, and outlier detection, with particular usefulness in high-dimensional spaces. [14]

The second model is a Quantum Support Vector Classifier. QSVC represents the quantum kernel-based part of the experiment. Instead of relying only on a classical kernel function, this approach uses a quantum kernel to map the input data into a quantum feature space. In Qiskit Machine Learning, QSVC is implemented as a classifier that uses a quantum kernel while keeping a familiar fit-and-predict workflow similar to classical machine learning models. [15] This makes it suitable for a comparative study, because it can be positioned close to the classical SVM baseline while introducing a quantum feature mapping mechanism.

The third model is a Variational Quantum Classifier. VQC represents the hybrid quantum-classical part of the experiment. It uses a parameterized quantum circuit whose output is interpreted as a classification result, while the parameters are adjusted through a classical optimization loop. According to the Qiskit Machine Learning documentation, VQC is a variational algorithm in which measured bitstrings are interpreted as classifier outputs. [16] In this study, the VQC model is included not because it is expected to outperform the classical baseline, but because it allows the experiment to examine how a variational QML approach behaves in a small-scale intrusion detection setting.

The implementation is carried out in a Kali Linux virtual machine using Python. Classical preprocessing and baseline modelling are performed with scikit-learn, while the quantum and hybrid models are implemented using Qiskit and Qiskit Machine Learning. Quantum execution is performed in a simulated environment rather than on real quantum hardware. This decision keeps the experiment reproducible and avoids additional variability caused by hardware noise, queue times, or backend availability. Qiskit Aer is suitable for this type of setup because it provides high-performance quantum circuit simulators and supports execution with or without noise models. [17]

TABLE 1 SUMMARY OF THE EXPERIMENTAL SETUP

Component	Description
Task	Binary intrusion detection
Dataset	Reduced and preprocessed NSL-KDD dataset

Classes	Normal traffic and attack traffic
Feature reduction	PCA to four components
Classical baseline	Support Vector Machine
Quantum model	Quantum Support Vector Classifier
Hybrid model	Variational Quantum Classifier
Environment	Kali Linux virtual machine
Main tools	Python, scikit-learn, Qiskit, Qiskit Machine Learning
Execution mode	Local quantum simulation

D. Evaluation Metrics

The models are evaluated using standard classification metrics and simple computational efficiency indicators. The selected performance metrics are accuracy, precision, recall, and F1-score. Accuracy provides a general view of the proportion of correctly classified instances, but it is not sufficient on its own for intrusion detection tasks. In IDS scenarios, the cost of different errors is not equal. A false negative may allow malicious activity to remain undetected, while a false positive may generate unnecessary alerts and increase the workload of security analysts. For this reason, precision, recall, and F1-score are included to provide a more balanced interpretation of model behaviour.

In addition to classification performance, training time and prediction time are measured. This is important because a model that achieves acceptable accuracy but requires disproportionate computational resources may be less suitable for practical intrusion detection. Runtime indicators are especially relevant in the context of QML, where simulation overhead can become significant even when the dataset is small. Therefore, computational efficiency is treated as part of the comparative evaluation rather than as a secondary implementation detail.

The results are planned to be presented through a summary table and several visual elements in the following section. These include a comparison of classification metrics, a comparison of execution times, and confusion matrices for the selected models. This combination of numerical and visual reporting allows the analysis to move beyond a single performance value and to discuss the models in terms of practical suitability, stability, and limitations. In line with the exploratory nature of the study, the results will be interpreted cautiously and will not be used to claim general quantum advantage. Instead, the experiment is intended to show how lightweight QML models can be tested, compared, and critically evaluated in the context of intrusion detection.

III. RESULTS AND DISCUSSION

The results reported in this section should be read as a compact experimental profile of the evaluated models rather than as a simple ranking by accuracy. The analysis therefore considers how each approach performs, how costly it is to execute, what types of errors it produces and how consistently it behaves across repeated runs.

A. Classification Performance of the Compared Models

The first part of the experimental evaluation focuses on the classification performance of the three selected models: the classical Support Vector Machine, the Quantum Support Vector Classifier, and the Variational Quantum Classifier. All models were trained and tested on the same reduced and pre-processed NSL-KDD subset, using a binary classification formulation with two classes: normal traffic and attack traffic. The dataset was balanced before training, and the feature space was reduced to four principal components in order to keep the comparison compatible with the lightweight quantum simulation setting.

The obtained results are presented in Table 2 and Figure 1. The classical SVM achieved the highest overall performance, with an accuracy, precision, recall, and F1-score of 0.9667. The identical values for these four metrics are the result of a balanced test set and a symmetric distribution of classification errors across the two classes. In other words, the model performed almost equally well in identifying both normal and attack instances.

TABLE 2 CLASSIFICATION PERFORMANCE OF THE EVALUATED MODELS

Model	Accuracy	Precision	Recall	F1-score
SVM	0.9667	0.9667	0.9667	0.9667
QSVC	0.9417	0.9649	0.9167	0.9402
VQC	0.8000	0.8103	0.7833	0.7966

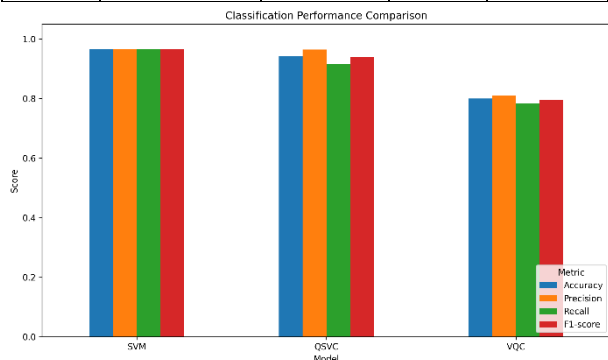


Figure 1 Classification performance comparison of SVM, QSVC and VQC

The QSVC model also produced competitive results, reaching an accuracy of 0.9417 and an F1-score of 0.9402. Its precision was slightly higher than its recall, which suggests that when the model predicted an attack, this prediction was usually reliable, but it missed a slightly larger number of attack instances than the SVM. This behaviour is important in intrusion detection, where recall has direct practical relevance because undetected attacks may remain active within a system.

The VQC model achieved lower performance across all classification metrics, with an accuracy of 0.8000 and an F1-score of 0.7966. Although this result is weaker than those of SVM and QSVC, it does not make the model irrelevant for the study. Rather, it shows that a hybrid variational quantum-classical approach can be implemented in a lightweight intrusion detection setting,

but its performance remains more limited and more sensitive to the constraints of the experimental configuration.

Overall, the classification results indicate that the classical SVM remains the strongest model in this experimental setting. QSVC appears promising from a predictive perspective, since its results are relatively close to the SVM baseline. However, the VQC results suggest that variational quantum models may require more careful tuning, larger repeated-run validation, or alternative circuit configurations before they can reach comparable performance in this type of task.

B. Computational Efficiency

Classification performance alone is not sufficient for evaluating intrusion detection models, especially when the task is associated with operational environments where timely detection is important. For this reason, the second part of the evaluation examines the computational efficiency of the three models. The comparison includes training time, prediction time, and total execution time, measured during the same experimental run used for the classification analysis.

The results shown on figure 2 show a clear difference between the classical and QML-based approaches. The classical SVM required only 0.0021 seconds for training and 0.0005 seconds for prediction, resulting in a total execution time of approximately 0.0026 seconds. This confirms its practical advantage as a lightweight baseline model. In contrast, the QSVC model required 224.59 seconds for training and 165.11 seconds for prediction, reaching a total execution time of 389.70 seconds. The VQC model required 30.73 seconds for training and 0.3055 seconds for prediction, with a total execution time of 31.03 seconds.

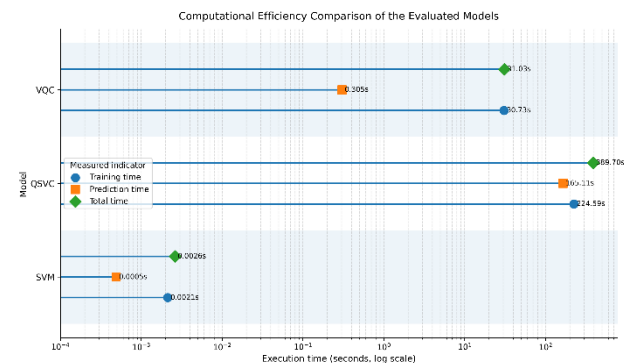


Figure 2 Computational efficiency comparison based on training, prediction and total execution time

These results reveal an important contrast between predictive quality and computational cost. QSVC achieved classification results relatively close to the SVM baseline, but this came with a substantial simulation overhead. Its total execution time was several orders of magnitude higher than that of the classical model. This difference is especially relevant for intrusion detection, where a model that performs well in terms of classification metrics may

still be difficult to justify if its execution time is too high for practical use.

The VQC model showed a different profile. It was clearly slower than the SVM, but considerably faster than the QSVC in this experiment. At the same time, its classification performance was weaker. This makes VQC an interesting but less competitive option in the present configuration. Its behaviour suggests that the hybrid quantum-classical approach may be computationally manageable in a small-scale setting, but further optimization would be necessary to improve its predictive performance.

Taken together, the computational results support the cautious interpretation adopted in this study. The quantum and hybrid models can be executed and compared in a lightweight simulated environment, but their practical value cannot be assessed only through accuracy or F1-score. In the present experiment, the SVM offers the best balance between performance and execution time, while QSVC demonstrates stronger predictive potential than VQC but at a much higher computational cost. This confirms that, under the current experimental constraints, the evaluated QML approaches are better understood as exploratory research models rather than immediately deployable intrusion detection solutions.

C. Error Distribution and Stability Analysis

To better understand the behaviour of the evaluated models, the analysis also considered the distribution of classification errors. This is particularly important in intrusion detection, where false negatives are more critical than ordinary classification mistakes, since they indicate attack instances classified as normal traffic. The confusion matrices for the three models are presented in Figure 3.

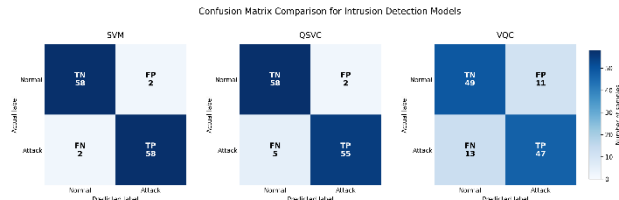


Figure 3 Confusion matrices for SVM, QSVC and VQC

The SVM model showed the most balanced error distribution, with 2 false positives and 2 false negatives. QSVC produced the same number of false positives, but a higher number of false negatives, misclassifying 5 attack samples as normal traffic. This explains its lower recall compared with SVM. The VQC model produced the weakest error profile, with 11 false positives and 13 false negatives, which confirms that its lower overall performance is not caused by a single isolated metric, but by a broader decline in classification reliability.

A repeated-run stability analysis was also performed using three different random seeds. The purpose of this step was to check whether the results remain consistent when the data split and sampling conditions change. The stability comparison based on F1-score is shown in Figure 4.

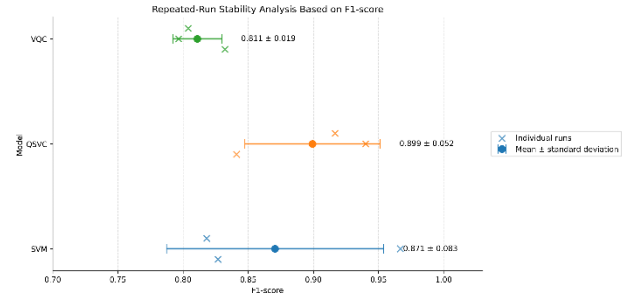


Figure 4 Repeated-run stability analysis based on F1-score

The repeated-run results showed that QSVC achieved the highest mean F1-score across the three executions, with a mean value of 0.8993 and a standard deviation of 0.0518. SVM followed with a mean F1-score of 0.8706, but with a higher standard deviation of 0.0833, indicating stronger variability across the repeated runs. VQC achieved the lowest mean F1-score, 0.8109, although its standard deviation was comparatively small at 0.0187. These results suggest that the single-run advantage of SVM should be interpreted together with the stability results, while QSVC appears more consistent in this reduced experimental setting despite its high computational cost.

D. Discussion of Practical Suitability

The results indicate that no model should be evaluated only through a single metric. The SVM model remains the most practical solution in the present setup because it combines high classification performance with extremely low execution time. Its main advantage is not only its accuracy, but the balance between predictive quality, speed, and relatively stable behaviour in the initial run.

QSVC is the most interesting quantum-oriented result. It achieved classification performance close to the classical baseline and showed the highest mean F1-score in the repeated-run analysis. However, this advantage is limited by the very high execution time observed during simulation. In practical intrusion detection, such computational overhead would be difficult to justify unless future implementations reduce the cost of quantum kernel evaluation.

The VQC model demonstrated that a hybrid quantum-classical classifier can be applied to the selected IDS task, but its results were less competitive. Its lower accuracy, higher number of false positives and false negatives, and weaker F1-score indicate that this configuration requires further tuning before it can be considered practically useful.

Overall, the findings support the main assumption of the study – lightweight QML models can be implemented and compared in an intrusion detection scenario, but the results do not demonstrate immediate quantum advantage. Instead, they show that QML methods are currently more suitable as exploratory research tools, while classical models such as SVM remain stronger candidates for practical deployment under constrained experimental conditions.

IV. CONCLUSION

This paper presented a lightweight comparative evaluation of classical, quantum, and hybrid quantum-classical machine learning models for intrusion detection. Using a reduced and pre-processed NSL-KDD dataset, the study compared SVM, QSVC, and VQC in terms of classification performance, computational efficiency, error distribution, and repeated-run stability. The applied value of the obtained results lies in providing a compact and reproducible evaluation procedure that helps identify the trade-offs between classification performance, computational cost, error behaviour, and stability before QML-based IDS approaches are considered for more realistic cybersecurity environments.

The results show that the classical SVM achieved the best balance between predictive performance and execution time. QSVC produced competitive classification results and demonstrated strong potential in the repeated-run analysis, but its high computational cost in the simulated environment limits its immediate practical applicability. VQC was successfully implemented as a hybrid quantum-classical model, but its performance remained weaker in the selected experimental configuration.

In conclusion, the findings do not indicate a clear quantum advantage in the examined intrusion detection scenario. Instead, they suggest that QML models should currently be understood as promising exploratory tools rather than direct replacements for established classical methods. Future work may extend this evaluation by using larger and more recent intrusion detection datasets, testing multiclass attack classification, exploring alternative quantum circuits, and comparing simulation-based results with executions on real quantum backends.

ACKNOWLEDGEMENTS

This article is the result of research funded by the National Science Fund of Bulgaria under project No. BG-175467353-2024-10-0013, contract No. KII-06-M87/5, dated December 6, 2024. The project is titled Artificial Intelligence and Cybersecurity: Navigating the Ethical Challenges.

REFERENCES

- [1] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1153–1176, Apr. 2016, doi: 10.1109/COMST.2015.2494502;PAGE:STRING:ARTICLE/CHAPTER.
- [2] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection".
- [3] "NSL-KDD." Accessed: May 10, 2026. [Online]. Available: <https://www.kaggle.com/datasets/hassan06/nslkdd>
- [4] "The UNSW-NB15 Dataset | UNSW Research." Accessed: May 10, 2026. [Online]. Available: <https://research.unsw.edu.au/projects/uns-nb15-dataset>
- [5] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature* 2017 549:7671, vol. 549, no. 7671, pp. 195–202, Sep. 2017, doi: 10.1038/nature23474.
- [6] J. Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018, doi: 10.22331/q-2018-08-06-79.
- [7] M. Cerezo *et al.*, "Variational quantum algorithms," *Nature Reviews Physics* 2021 3:9, vol. 3, no. 9, pp. 625–644, Aug. 2021, doi: 10.1038/s42254-021-00348-9.
- [8] M. Schuld and N. Killoran, "Quantum Machine Learning in Feature Hilbert Spaces," *Phys. Rev. Lett.*, vol. 122, no. 4, p. 040504, Feb. 2019, doi: 10.1103/PhysRevLett.122.040504.
- [9] V. Havlíček *et al.*, "Supervised learning with quantum-enhanced feature spaces," *Nature* 2019 567:7747, vol. 567, no. 7747, pp. 209–212, Mar. 2019, doi: 10.1038/s41586-019-0980-2.
- [10] F. Pedregosa FABIANPEDREGOSA *et al.*, "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, no. 85, pp. 2825–2830, 2011, Accessed: May 10, 2026. [Online]. Available: <http://jmlr.org/papers/v12/pedregosa11a.html>
- [11] G. Aleksandrowicz *et al.*, "Qiskit: An Open-source Framework for Quantum Computing", doi: 10.5281/ZENODO.2562111.
- [12] "GitHub - qiskit-community/qiskit-machine-learning: An open-source library built on Qiskit for quantum machine learning tasks at scale on quantum hardware and classical simulators · GitHub." Accessed: May 10, 2026. [Online]. Available: <https://github.com/qiskit-community/qiskit-machine-learning>
- [13] N. Institute of Standards, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," 2020, doi: 10.6028/NIST.AI.100-1.
- [14] A. J. Smola and B. Schölkopf, "A tutorial on support vector regression," *Stat. Comput.*, vol. 14, no. 3, pp. 199–222, Aug. 2004, doi: 10.1023/B:STCO.0000035301.49549.88.
- [15] "QSVC - Qiskit Machine Learning 0.9.0." Accessed: May 10, 2026. [Online]. Available: https://qiskit-community.github.io/qiskit-machine-learning/stubs/qiskit_machine_learning.algorithms.QSVC.html
- [16] "VQC - Qiskit Machine Learning 0.9.0." Accessed: May 10, 2026. [Online]. Available: https://qiskit-community.github.io/qiskit-machine-learning/stubs/qiskit_machine_learning.algorithms.VQC.html
- [17] "Qiskit Aer 0.17.1." Accessed: May 10, 2026. [Online]. Available: <https://qiskit.github.io/qiskit-aer/>

Comparative Analysis of Motivational Factors for Service in the Bulgarian Armed Forces (2017–2025)

Teodora Grozdanova

Defence Advanced Research Institute
Rakovski National Defence College,
Sofia, Bulgaria
t.grozdanova@mdc.bg

Abstract: This study focuses on the dynamics of motivational factors for service in the Bulgarian Armed Forces. It aims to guide management policies toward enhancing motivation and retention of personnel within the context of a constantly changing security environment.

The analysis is based on a cross-sectional study of two independent representative samples of military personnel. Each of them comprises of approximately 1,500 respondents. Primary data were collected through a direct anonymous survey conducted within two representative empirical sociological studies of the Bulgarian Armed Forces. The latter were carried out in 2017 and 2025, respectively. The period between the two surveys provides a relatively broad time horizon for conducting a comparative analysis of mean values and the rank structure of motivational factors.

The results indicate an increased significance of factors related to social security, remuneration, and the balance between professional and personal life. At the same time, there is a gradual decline in the influence of traditionally dominant internal motivators for service. The observed dynamics reflect the impact of the changing institutional and socio-economic environment on the motivational priorities of the military personnel.

The study provides up-to-date empirical data on the transformation of military personnel's motivational attitudes, in which the amount of remuneration, job security and the balance between professional and personal life are of leading importance.

Recommendations from the analysis include the introduction of personalized incentives, improvement of social benefits, and systematic monitoring of motivational trends to update motivation strategies and human resource management policies. Aligning management practices with the factor structure of military personnel's motivational attitudes contributes to personnel retention, enhances

individual and organizational effectiveness, and strengthens operational readiness within the national security and defence system.

Key words: Bulgarian Armed Forces, comparative analysis, motivational factors, sociological studies.

I. INTRODUCTION

Human resource management is a complex process, as all activities within its system are interconnected, while each organization operates both within its internal environment and under external environmental conditions. In the academic literature, human resource management is defined as a specific management activity aimed at attracting, retaining, motivating, developing, and utilizing the people necessary for the organization's operations. It encompasses the following key elements: job analysis and design, human resource planning, personnel selection, training and development of human resources, performance appraisal, compensation and benefits, and ensuring safe and healthy working conditions [1], [2], [3].

Motivation is a continuous process involving the use of various tools and approaches, the purpose of which is to stimulate people's willingness to perform their tasks effectively and with commitment [4]. Motivation occupies a central place in organizational management, and as it enables organizations not only to exist but also to achieve high performance.

The theories of Abraham Maslow, Frederick Herzberg, and Victor Vroom are regarded as socio-psychological approaches to the study of motivation. According to Abraham Maslow's theory of the hierarchy of needs (the Hierarchy of Needs), human behaviour in organizations is driven by the desire to satisfy needs arranged in a hierarchical structure. The transition to satisfying higher-

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.124>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

order needs occurs only after lower-level needs have been fulfilled [5].

According to Frederick Herzberg's two-factor theory, the conditions influencing individual motivation are divided into two main groups – hygiene/external (working conditions, salary, job security, interpersonal relations) and motivators/internal factors (achievement, recognition, responsibility, and opportunities for development). According to Herzberg, only internal factors lead to true motivation, while external can only prevent dissatisfaction [6]. While Maslow's theory emphasizes the hierarchical structure of motivational factors, Herzberg's approach focuses on distinguishing between true motivators and those that merely create basic working conditions.

Victor Vroom's expectancy theory views motivation as a result of conscious choice, explaining how individuals select behaviour that they believe will lead to desired outcomes such as recognition or professional development, higher income, and security [7].

The presented theoretical approaches do not fully cover the topic of motivation, given its specific characteristics in the military context. In the scientific literature, three main approaches stand out, which examine the motivation of military personnel from different perspectives. In his studies, Morris Janowitz Segal views the military institution as a specific social system in which the motivation is formed not so much by individual needs, but is based on values such as mission, duty, morality, and commitment to a collective cause. This orientation builds a strong professional identity and a high degree of commitment to the institution and service in the public interest [8].

For Samuel Huntington, the army is an autonomous professional organization, and the motivational factors are rooted in professional ethics. Officers are motivated by their commitment to the profession and by a sense of duty to society to apply their professional expertise in its service [9].

Originally formulated in the late 1970s Moskos' model of the transformation of the armed forces proposes that contemporary armies are shifting from an "institutional" to an "occupational" (professional-organizational) type, a process that leads to changes in the motivation of military personnel [10]. In the occupational model, the military increasingly resembles the civilian labour market, and motivation is based on a cost–benefit ratio with a clearly career-oriented focus. Moskos argues that the motivation in the armed forces is mixed – partly value-based (duty, mission) and partly pragmatic (pay, security, status). He further emphasizes that military motivation cannot be reduced either to a purely value-based "calling" or to a market-oriented career, but rather represents a dynamic combination of institutional and professional incentives that evolves over time [11].

The synthesis of the theoretical approaches indicates that motivation is a multifaceted process aimed at the selection, direction, and regulation of human behaviour, thereby ensuring both flexibility and persistence in goal

attainment. Within the military context, the motivation can be conceptualized as an outcome of socialization and organizational integration, reflecting professional ethics, domain-specific expertise, and a deeply internalized sense of duty. It further represents a dynamic interplay between institutional values and pragmatic, career-oriented incentives. Accordingly, the motivation of military personnel should be understood as a complex, multifactorial phenomenon with a dynamic nature, shaped by developmental processes both within the military organization and within society as a system.

The reviewed theoretical approaches suggest that the complexity of soldiers' motivation is shaped by the interaction between institutional and career-oriented pragmatic factors. In this context, a comparative analysis of empirical findings was undertaken to evaluate the actual motivational drivers of military personnel and to assess the extent to which these findings support or refine the proposed theoretical models.

On this basis, the study formulates the hypothesis that, as a result of socio-economic and organizational transformations over the past decade, the importance of career-oriented pragmatic motives has increased relative to institutional ones. At the same time, institutional motives have not been entirely reduced; rather, their relative weight within the overall motivational structure has declined.

II. MATERIALS AND METHODS

The analysis is based on a cross-sectional study of two independent representative samples of military personnel, each comprising approximately 1,500 respondents. Both samples were constructed to reflect the structure of the Armed Forces of the Republic of Bulgaria, thereby ensuring comparability and methodological consistency across the two time points.

Primary data were collected through a direct anonymous survey conducted within two empirical sociological studies in 2017 and 2025. The survey instrument included standardized items measuring the importance of selected motivational factors for military service, assessed using a Likert-type scale.

A structured sampling procedure was applied to ensure adequate representation of different ranks, service branches, and categories of military personnel. This approach enabled balanced coverage of the main subgroups within the military population and contributed to the external validity of the findings.

The time interval between the two surveys provides a robust temporal basis for comparative analysis of both mean values and rank order distributions of motivational factors. This design enables the identification of structural changes in motivational priorities over time.

Data analysis was conducted using descriptive statistical methods, including the calculation of arithmetic means and rank ordering of motivational factors. A comparative approach was applied to examine differences between the two time points (2017 and 2025), enabling the identification of trends in the motivational structure.

III. RESULTS AND DISCUSSION

The analysis of military personnel's assessments of the importance of motivational factors for service in the Bulgarian Armed Forces is presented in Table 1.

TABLE 1

	Assessments of motivational factors		
		Mean score 2017	Mean score 2025
1.	Amount of remuneration	4.31	4.43
2.	Secure and guaranteed employment position	4.36	4.42
3.	Desire to serve my country	4.40	4.36
4.	Opportunity to improve professional skills	4.24	4.22
5.	Opportunity for early retirement	4.05	4.21
6.	Interest in the specific field of work	4.11	4.19
7.	Opportunity for more annual vacation time	3.89	4.16
8.	Opportunity for a professional career	4.00	4.07
9.	Interest in military equipment, armament, and technologies	4.03	4.03
10.	Social prestige of the military profession	3.90	3.79
11.	The challenges of the military profession	3.74	3.59
12.	Desire to be a leader, to command and manage others	3.51	3.48
13.	Opportunity to participate in international missions	3.41	3.08
14.	Opportunity to use service accommodation	2.95	2.95

Note: Rating scale: 1 – “not important at all”, 2 – “rather not important”, 3 – “neither yes nor no”, 4 – “rather important”, 5 – “very important”.

A comparative analysis of military personnel's evaluations of career development motives between 2017 and 2025 reveals relatively high mean values (most exceeding 4.00), indicating that these motives remain consistently and strongly important over time. The retrospective examination of the results reveals certain dynamics in the motivational structure, reflecting a hierarchical shift characterized by strengthening of some motives, the weakening of others, and the stability of a third group.

The most strongly motivating factors for career development among the surveyed respondents include the amount of remuneration (4.43), a secure and guaranteed employment position (4.42), the desire to serve one's country (4.36), as well as opportunities for improving professional skills (4.22), early retirement (4.21), and interest in the specific field of work (4.19).

Motives with a moderate level of importance are ranked as follows: the challenges of the military profession (3.59),

and desire to assume leadership roles and command and manage others (3.48).

The least important motives are the opportunity to use service accommodation (2.95) and participation in international missions (3.08).

The analysis of the obtained evaluations regarding potential factors influencing these results does not reveal statistically significant differences in respondents' answers, while the motivation of military personnel to serve in the Armed Forces of the Republic of Bulgaria is assessed as relatively high (3.97).

The comparative analysis of the results relative to 2017 indicates an increase in the importance of pragmatic factors such as financial-material incentives and the need for a secure and stable employment position. A significant increase is also observed in motivational factors such as the opportunity for longer annual leave and early retirement.

Relatively unchanged, but still high, are the evaluations of motives such as interest in military equipment, opportunities for career advancement, and the desire to serve one's country.

The analysis of the rank distribution of motives within the motivational structure indicates an increase in the importance of factors such as financial-material incentives and job security and stability. An increased relative weight is also observed for motives related to longer annual leave and early retirement, indicating a stronger need for a balance between professional and personal life [12]. The decline in the importance of factors such as social prestige, the challenges of the military profession, and the opportunity to participate in international missions indicates a shift in priorities toward greater stability and predictability of the working environment.

The opportunity to use service accommodation remains the factor with the lowest level of importance, showing no change in its evaluation compared to ten years ago. This result confirms the dominant role of financial and material security as a motivational factor relative to the provision of service accommodation, which is likely perceived as a supplementary or more neutral element, as it is considered rather a component of the institution's social policy than a determining motive for choosing the military profession.

The obtained results confirm the main research hypothesis regarding the increasing importance of career-pragmatic motives within the motivational structure. At the same time, no decline in institutional motives is observed, as their significance remains stable over the examined period. This result is highly consistent with Charles C. Moskos' institutional-occupational model, which allows for a dynamic balance between institutional values and career-pragmatic incentives without implying their mutual exclusion.

IV. CONCLUSIONS

The analysis of empirical data reveals a strengthening of pragmatically oriented motives among military personnel during the period 2017–2025. Leading factors

for career development remain material and financial incentives and job security, the importance of which has increased and continues to dominate over patriotic and leadership motives.

At the same time, interest in professional development and military technology remains relatively a stable, suggesting that professional identity continues to play an important role within the armed forces. In contrast, a decline in the importance of participation in international missions is observed, which may be interpreted as a reorientation of priorities toward internal stability and predictability of service conditions.

Both empirical studies indicate that existential needs—primarily income and stability—represent a key driver of military personnel motivation. In this context, the results align with the Institutional–Occupational Model proposed by Charles C. Moskos, which emphasizes the dynamic balance between institutional values and career-oriented pragmatic incentives within the armed forces.

V. RECOMMENDATIONS

At the end of 2025, as a result of the policy efforts of the leadership of the Ministry of Defence and the Armed Forces the Strategy for the Motivation of Personnel was completed. The Strategy aims to provide a comprehensive and systematized framework for attracting, developing, and retaining qualified personnel, with expected outcomes including increased attractiveness of military service, improved personnel retention, and enhanced levels of professional development among service members in the Armed Forces.

The recommendations from the study focus on the introduction of personalized incentives, improvement of social benefits, and systematic monitoring of motivational trends in order to update the motivation strategy and human resource management policies [13], [14], [15]. Aligning management practices with the motivational structure will contribute to higher job satisfaction, personnel retention [16], improved efficiency and effectiveness, and strengthened operational readiness within the national security and defence system.

In conclusion, the sustainable development of the motivation system in defence requires a comprehensive and balanced approach that integrates internal and external motivational factors, such as material incentives, professional development, and institutional affiliation, thereby contributing to more effective personnel management within the military organization.

VI. ACKNOWLEDGMENTS

The report was developed in implementation of the National Scientific Programme “Security and Defence”, adopted by Council of Ministers Decision No. 731 of 21.10.2021, and in accordance with Agreement No. D01-74/19.05.2022, financed by the Ministry of Education and Science of the Republic of Bulgaria.

REFERENCES

- [1] M. Atanasova, *Human Resource Management: Theory and Practice*. Sofia, Bulgaria: Avangard Prima, 2015.
- [2] D. Tashkov, E. Pavlova, V. Gagamova, and V. Vasileva, “Analysis of Cybersecurity Training Platforms and Simulation Environments and Opportunities for Their Integration into Higher Education,” in *Proc. 31st Int. Conf. Knowledge-Based Organization (KBO)*, vol. 3: *Applied Technical Sciences and Advanced Military Technologies*, Sibiu, Romania, 2025, pp. 177–181, <https://doi.org/10.2478/kbo-2025-0094>.
- [3] V. Aleksandrova, A. Guncheva, and V. Vasileva, “Technological Solutions Supporting Modern E-Learning,” in *Proc. 7th Nat. Conf. E-Learning in Higher Education*, Sofia, Bulgaria, 2018, pp. 216–223. Sofia, Bulgaria: University Publishing House “St. Kliment Ohridski,” 2018.
- [4] *Encyclopedic Dictionary of Sociology*. S. Mihaylov, Gen. Sci. Superv. and Ed.; N. Tilkidzhiev, Comp. and Ed. Sofia, Bulgaria: M-8-M, 1997.
- [5] A. H. Maslow, “A Theory of Human Motivation,” *Psychological Review*, vol. 50, no. 4, pp. 370–396, 1943, <https://doi.org/10.1037/h0054346>.
- [6] F. Herzberg, B. Mausner, and B. Snyderman, *The Motivation to Work*. New York, NY, USA: John Wiley & Sons, 1959.
- [7] V. H. Vroom, *Work and Motivation*. New York, NY, USA: Wiley, 1964.
- [8] M. Janowitz, *The Professional Soldier: A Social and Political Portrait*. New York, NY, USA: Free Press, 1960.
- [9] S. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations*. Sofia, Bulgaria: Ministry of Defense Publishing House “St. George the Victorious,” 1998.
- [10] C. C. Moskos, “Institutional/Occupational Trends in Armed Forces: An Update,” *Armed Forces & Society*, vol. 12, no. 3, pp. 377–382, 1986.
- [11] C. C. Moskos, J. A. Williams, and D. R. Segal, Eds., *The Postmodern Military: Armed Forces after the Cold War*. Oxford, U.K.: Oxford University Press, 2000.
- [12] T. V. Georgieva, *Socio-psychological problems of military families: A monograph*. Sofia, Bulgaria: Vidzhi – Viktor Gutsev, 2022.
- [13] V. Aleksandrova, V. Tagareva, and V. Vasileva, “Regarding the Needs for Knowledge and Artificial Intelligence as a Guarantee for the Change of Modern Bulgaria: Ethical Aspects of the Application of Artificial Intelligence in Autonomous Systems,” in *Proc. XVIII Int. Conf. Open and Underwater Mining of Minerals*, Varna, Bulgaria, 2025, pp. 225–234. Sofia, Bulgaria: Scientific and Technical Union of Mining, Geology and Metallurgy, 2025.
- [14] V. Vasileva and V. Gagamova, “Raising Cyber Awareness for Users from Public Sector Organizations to Improve Ethical Behavior in the Virtual World,” in *Proc. 16th Int. Conf. Educ. New Learn. Technol. (EDULEARN)*, Palma, Spain, Jul. 1–3, 2024. Valencia, Spain: IATED, 2024, pp. 10167–10171, <https://doi.org/10.21125/edulearn.2024.10167>.
- [15] V. Vasileva and V. Gagamova, “Application of the Simulation Modeling in Education and Scientific Research: An Exploration Through Predictive Scenarios of Cybersecurity Threats,” in *Proc. 18th Int. Conf. on Education, Research and Innovation (ICERI)*, Seville, Spain, Nov. 10–12, 2025, pp. 8962–8969. Valencia, Spain: IATED, 2025, <https://doi.org/10.21125/iceri.2025.2527>.
- [16] N. Boteva, “Attitude towards work in organization,” *International Journal of Scientific and Applied Research*, vol. 9, pp. 31–35, 2016.

AI-Driven Model for Economic Efficiency in Software Development Tasks

Viktor Hristov

Management Department
University of National and World Economy
Sofia, Bulgaria
viktor.hristov@unwe.bg

Miglena Angelova

Management Department
University of National and World Economy
Sofia, Bulgaria
m.angelova@unwe.bg

Abstract— The use of Artificial Intelligence (AI) has become an inseparable part of the software development process, parts of which are routine, requiring precision rather than creativity. AI code generation speeds up productivity by automatically completing code fragments and frees up time and brainpower to perform more tasks that require creativity or problem-solving. When writing code, the programmer uses not only the accumulated experience, but often also intuition, which helps him assess both the correctness of the code and the implications of its use.

At the same time, AI uses different and increasingly sophisticated models and a thought chain resembling human thinking through modern approaches to Large Language Models (LLM) and Neural Networks. However, increasingly serious problems are emerging when using AI.

The publication proposes a model of an AI algorithm with two functionally different cores: one creative and one process, including control functions. This model overcomes a large part of the identified shortcomings of AI and complements their development. The model is supplemented with quantitative metrics to determine the economic efficiency of its application.

Keywords— Artificial Intelligence, Economic Effectiveness, Two core AI model

I. INTRODUCTION

AI becomes increasingly integral part of activities in software development companies. It spreads over vast activities in Software Development Life Cycle and automatizes activities like Project Management, Coding and Quality Assurance. Still efficiency of AI assisted or committed tasks is yet to be confirmed.

II. LITERATURE REVIEW

The broad academic discussion about the benefits of using Artificial Intelligence is extremely lively and has enjoyed the attention of researchers in recent years, especially after the widespread penetration of AI into work

and personal life. Respectively, the use of AI in software development and work on software tasks is also an issue on which a multi-layered discourse is currently underway. Scientists are studying various aspects - in terms of efficiency and productivity, achieved level of quality and reliability, security and potential risk, interaction between humans and AI, management and decision-making, Algorithmic Management, purely economic dimensions of AI in software development, etc.

In this context, the role of artificial intelligence extends beyond isolated applications and increasingly encompasses the full lifecycle of software development. Revuri, Sakthivel and Nagasubramanian [1] acknowledge that artificial intelligence is radically transforming software development, introducing a higher degree of automation, which in turn leads to increased productivity. The scholars argue that through applications such as automatic code generation, error detection and test creation, AI improves the efficiency and quality of development at all stages of the SDLC, while preserving the primary role of human creativity.

This systemic integration of AI naturally leads to transformations not only in processes but also in the way software development activities are structured and executed. De La Cruz et al. [2] state that artificial intelligence is radically changing the way programmers work. The increasing and increasingly ubiquitous use of AI tools naturally requires the possession and development of new skills, instead of just focusing on writing code, as before. At the same time, scientists explicitly specify that these tools are not completely reliable and can lead to errors, so it remains important for a person to check and control the results.

According to a study by Kumari et al. [3], artificial intelligence is integrated into all stages of software development, with the main advantages being that it automates routine activities and contributes to increasing productivity, quality, and speed of development. They see

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.177>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

AI as a major opportunity to increase the efficiency of modern software processes.

Beyond general improvements in productivity and speed, more granular analyses focus on the specific mechanisms through which these effects are achieved. Adnyana and Schwung [4] comment that the application of generative AI models to the creation of program code leads to a significant reduction in the effort required for subsequent corrections and to an improvement in the quality of the results. In addition, it is highlighted that the way the instructions are formulated has a greater impact on the accuracy and reliability of the generated code than the choice of a specific model.

Complementing these findings, other studies emphasize that the effectiveness of AI is not uniform, but contingent upon technological and organizational alignment. Banh, Holldack, and Strobel [5] argue that generative AI has the potential to increase productivity in software development. However, they emphasize that its successful implementation depends on the alignment of technological capabilities, organizational practices, and the way developers themselves work.

This line of reasoning is further reinforced by comparative analyses of different types of AI solutions. According to Bañuls-Lapuerta et al. [6], the effectiveness of generative AI models in software creation varies significantly depending on the type of model used, with paid solutions demonstrating higher accuracy and less need for additional interactions.

In addition to general development processes, AI demonstrates strong applicability in specific functional domains of software engineering. According to Czarnacka-Chrobot [7], the application of artificial intelligence in the processes of measuring the functional size of software leads to a reduction in subjectivity and labour intensity, while improving the accuracy and reproducibility of estimates. This creates the real prerequisites for more reliable planning of the efforts, costs and duration of software projects.

Similarly, the role of AI becomes particularly visible in higher-level decision-making processes within software development. Esposito et al. [8] claim that generative AI has a very good application in software architecture processes, especially in making architectural decisions and transforming requirements into code. However, they also note that there is currently a lack of established methods for evaluating the results, which limits the possibilities for objectively assessing its effectiveness.

However, alongside these benefits, the integration of AI introduces a set of critical challenges related to security and reliability. According to Glas et al. [9], generative artificial intelligence increases the efficiency of software development, but at the same time creates significant security risks, mainly related to the unreliability of the generated code and excessive trust of developers. Scientists are of the opinion that its effective use requires a human-centred approach that allows for the use of the technological capabilities of AI but retains human control and critical assessment.

These concerns are further expanded in studies focusing on secure software development practices. Al-Hashimi et al. [10] conclude that generative AI is increasingly being used in practice as a means of improving security in the development process, especially by detecting vulnerabilities and supporting secure programming. On the other hand, researchers also pay significant attention to the fact that its implementation creates new challenges related to reliability, ethical risks, and integration into existing processes.

At a more advanced level, the discussion extends to the need for explainability and transparency in AI-driven systems. Basheer et al. [11] comment that modern approaches to vulnerability detection using artificial intelligence place emphasis not only on accuracy. The same importance should be paid also on explainability, reliability, and security of models. This leads to the conclusion that effective application of AI in software development requires a professional combination of high performance with transparency and control.

Despite the increasing level of automation, the human factor remains central in determining the effectiveness of AI applications. In this line of consideration, it should be noted that a study by Shao and Ishengoma [12] shows that the use of generative artificial intelligence in software development depends largely on people – on their experience, attitudes and the influence of the environment around them. Furthermore, there are clear differences between the way students and professionals work with these tools, which in turn leads to the conclusion that the effects of AI are not the same for everyone.

This observation aligns with comparative perspectives on human–AI collaboration. Ampatzoglou et al. [13] conduct a comparative analysis between AI-assisted and fully human solutions. They come to the idea that there is a clear distinction between the two approaches: AI significantly supports the process for more precise task execution, but on the other hand, human intervention remains indispensable in recognizing problems and making quality decisions.

At the same time, the current stage of development of AI-based systems reveals a number of structural limitations. Giray [14] concludes that the development of machine learning-based systems is characterized by a high degree of complexity and non-determinism, with a lack of established engineering practices and tools in several areas. It is also found that despite growing interest, existing solutions are often at an early stage of development and have not been sufficiently validated in a real environment.

From a broader organizational perspective, the application of AI extends beyond software development to encompass core business processes. Anguelov [15] takes a more conceptual approach to the use of AI in business organizations. According to the author, the application of artificial intelligence in enterprise resource management systems covers a wide range of organizational processes, including supply chain management, financial activities, and human resources. Therefore, it can be concluded that

AI is used as a tool for optimization and automation of various business functions.

Within this evolving landscape, the question of how to evaluate the efficiency of AI-supported software development tasks becomes increasingly significant, particularly in the context of model-based and predictive approaches. In the development of AI-based models, the essential role of the indicators used is highlighted. According to Anguelov [16], their selection directly affects the accuracy of the results. In this logical sequence of reasoning, it can be assumed that in the assessment of the effectiveness of software tasks, the selection and structuring of indicators is decisive for the reliability of the predictive function of the model.

The aforementioned studies clearly show that artificial intelligence can significantly increase the efficiency of software development. However, it should also be noted that its impact is mediated by technological, organizational and human factors. This necessitates the development of structured, indicator-based approaches to ensure the reliability of the predictive function of AI-powered models.

III. AI SPECIFICS AND WEAKNESSES

Machine Learning (ML) process has following group of activities: *Model Requirements*, *Input data* (collection/preparation/processing), *Feature engineering*, *Model training and evaluation*, *Deployment and maintenance* [17]. Input data and the phenomenon of data cascades show their elevating importance to AI efficiency [18]. It can also lead to inaccurate and biased results [19] or to spread in the model errors like so called silent failures [20]. Improving data quality should be done if possible before the data is inserted into AI model. Furthermore, internal mechanism for data correction should be available, which for AI based on Neural Network (NN) system is a process called backpropagation.

There are many scientific articles which point to the central role of learning algorithms in AI systems. Few authors [21], [22], [23] point out in different ways importance of learning algorithm to AI. Core of learning methodology and algorithms lies in different theories, most of them focused on the ability of the model to predict accurate as possible results and optimization of that process. Empirical risk minimization [24] or Bias-Variance Tradeoff [25] are even more directly aimed on that. There are additional optimization theories like Convex Optimization Optimality [26], [27], which address optimal (shortest) paths for dynamic programming. Reinforcement Learning and Bayes Optimality (Probabilistic Learning) offers decision rules under uncertain environment. Emphasis on all of them is to minimize errors and predict accurate as possible results. However, that process could slow down performance and does not consider efficiency. Successful implementation of learning algorithms depends on the supervision of learning process, which can be done via human interactions. This process is known as Human in the loop (HITL). HITL implementation in Reinforcement learning model brings valuable contribution.

All these methods are essential to learning algorithm optimization and reducing the errors, but it does not consider how effective outputs are. We acknowledge that some tasks in software development are still handled more effectively by humans, for example: naming conventions and redefinition of variables, more high severity errors in the code uncomplete code documentation [28]. Y. Liu et al. [29] are pointing that it is “very unlikely” all AI generated code has been reviewed by human, and thus there could be unrevealed errors, including security vulnerabilities. Above authors’ analysis is discovering three types of violation done by AI assisted coding: *Code smells*, *Runtime bugs* and *Security issues*, with comparison results that AI assisted coding can reduce the time needed to fix maintenance issues and to generate simple and repetitive patterns. Committed field experiment also confirmed that for “easy and medium-level problems” AI enhances the performance of coding solutions compared to novice programmers’ output [30].

As one of the conclusions of challenges in front of AI assisted systems marked above, we see that sometimes it is more efficient to use human resources or to put humans in the loop instead of relaying on AI fully automated processes. If that interaction is unnecessary often it will decrease overall efficiency of AI implementation. In addition, drawbacks that put obstacles across successful AI implementation are:

- *Underestimated optimum properties in terms of economic efficiency*
- *Possibility for peak loading and performance degrade*

IV. AI TWO CORE CONCEPT

A. Description

The AI two core concept encompasses first core conditionally named *Creative*, and second core named *Operative*. First core is dedicated to creative intensive tasks it is based on modern learning techniques. Second core has variable sets of rules and dictionaries, and it will maintain control functions as well. From another point of view Creative core can be seen as microprocessor maximum configuration, Operative – as minimal [31]. Based on stochastic and classical learning model Operative core maintains stable sets of proven solutions, optionally some of them marked with calculated economic efficiency coefficient (*EEC*) [32]. Creative core is designed to pass all prompts to Operative Core. If results are already available there Operative Core will return them back together with optionally calculated *EEC*, and it will do validation operations to avoid violations (code review for example).

Every user prompt goes to Creative core that automatically passes it to Operative Core which holds previous results and *EEC* [33]. It also monitors learning and processing operations in Creative Core, and if its resources are fully loaded or prompts are repeating, it triggers automatically human interventions. Operative core has the duty to avoid repeating answers or hallucinations

possibly done by Creative Core and automatically supervise its answers, and vice versa – Creative Core validates all results generated by Operative core. If there is a conflict, orchestrator triggers HITL interventions. Operative core also stores the data about previously executed tasks marked as effective economically with their respective *EEC* [34].

General diagram of the concept is presented on “Fig. 1” and descriptions of some characteristics are noted in “Table 1”.

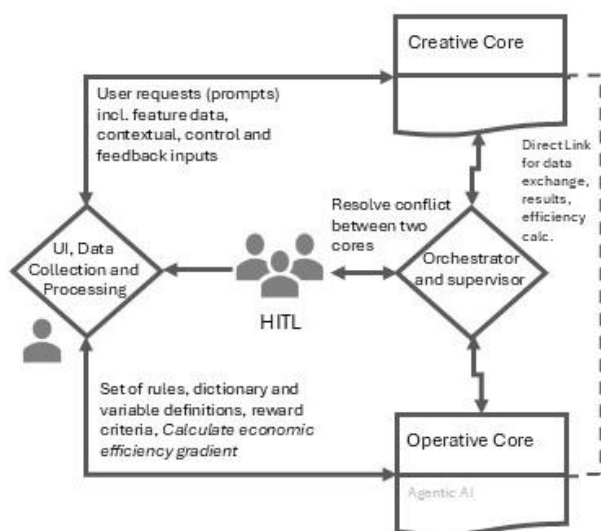


Fig. 1. Two core concept diagram

Sometimes learning and prediction could tend to use enormous learning steps, with very large number of passes. Learning algorithms could also tend to be unvaluable from economic perspective. To avoid that, authors propose to use dynamically calculated dedicated bias coefficient incorporated in all learning algorithms - *EEC*. The role of *EEC* is to put conditions to pass or prevent upon AI decisions. It is designed to adjust boundaries of the decision just like regular bias coefficient, with the difference it will be dedicated only for the purpose and set as optional attribute. In other words, it is bias factor which will decide which task to be executed by AI and which by human. It can also serve to distribute work between two cores and to assign more resources to economically valuable user prompts.

B. Use of EEC

EEC is calculated for functions with low level of Conditional entropy ($H(Y | x) \rightarrow \min$). Smallest independent unit of work done by AI should have its own economic coefficient c that is obtained from previous experience (or learning cycle). By independent unit we understand that all its elements or components have equal significance by each other. *EEC* is a sum of all economic coefficients (c_n) managed for more complex tasks or project phases. It can be designed to be calculated by ML with HITL interactions. The values of c can be adjusted based on the nature of the task and/or previous knowledge and experience.

$$eec = c_1 + c_2 + \cdots c_n \quad (1),$$

where c_n is indexed economic coefficient of smallest independent task

EEC is integrated in learning algorithms, for example of backpropagation:

$$z = w_1x_1 + w_2x_2 + \cdots + w_nx_n + meec \quad (2)$$

if $z > R$ then $a = f(z)$ else null end (3),

where z – computational unit; x – inputs, w – weights, $a, f(z)$ – activation function, R – reference value, $_{m}eec$ – normalized value of eec .

Normalization rules need to be defined later, but as general guideline authors propose weight of *eec* should be no more than 15% of value of backpropagation equation. Populated value of z is used only to compare with human defined boundaries and trigger or reject activation function. The more complex the task is, the more efficient will be the algorithm.

Example: we have AI assisted development task A consisted of two subtasks A1 (generate drop-down menu in UI) with $c = 5$ and A2 (button with submit action) with $c = 7$. Coefficients are calculated based on previous experience and c is ranked [1..10], 1 - means very ineffective and needs a consideration to be done solely by human, 10 - means perfectly executed by AI. The assessment is done entirely from economic point of view. EEC for task A is calculated as average value of A1 and A2 (equal significance). $EEC = 6.5$. This value is added into backpropagation after normalization. We know from previous experience that z minus eec is 60. We set R for A task at level 70. That means activation function will not be triggered, and we change x inputs and their respective w in order to achieve economic efficiency and trigger activation function. During the time x and w can be changed, eec will remain the same unless specific input for it is provided by humans or dedicated learning algorithm. In other case z can become “economic ineffective” and inputs needs to be changed anyway (for example do not ask AI to create button with specific action).

Activation function is enabled only if neuron value is above parametrized boundary values stored in Operative core.

TABLE 1 CONCEPT MAIN ELEMENTS OVERVIEW

Two Core Model	Purpose	Learning Methods	Expected output	Data source	Human Supervised
Creative Core	Handle all creative tasks, continuous learning with human supervised Deep Learning and Neural Network models	Supervised fine-tuning; Reinforced Learning from Human Feedback; Preference Optimization; Diversity-aware preference; Generative Adversarial Networks	Creative, out of the box solutions; complex tasks solution; code new features	Live data, Human labelled data, adaptive data modification	Yes, during learning process
Operational Core	Handle all repeating complex or all simple tasks, interested	Linear Regression or Classification; Support Vector Machine (SVM);	Check and validate code, monitor and distribute	Verified results from Creative Core	No, only parameters modification

Two Core Model	Purpose	Learning Methods	Expected output	Data source	Human Supervised
	supervisory controls, KPIs, AI agents for task distribution, calculating R	Kernel SVM; k-Nearest neighbor; Decision Tree	tasks between teams, Compute control samples	stores all data about definitions and variables	

C. Advantages of the concept

- *Enable secure validation of AI output:* one core can be more open to getting large and complex data with state of art algorithms thus more exposed to external threats, while second one can be more encapsulated which will directly control output of the first core and in case of colliding or conflicting results to trigger human in the loop interventions. As an example, AI tend more to hard code API passwords which can be fixed directly during code generation by operational core.
- *Ensure monitoring of economic effectiveness:* real-time direct supervision of results and controlling.
- *Distribute work in efficient and programable way:* tasks are passing through creative core, which is handling only complex and generative ideas, the rest like daily work distribution are passed to Operative core.
- *Reduce human supervision and promote it as final control point:* it provides substitution for some of human supervised learning tasks.

V. CONCLUSION

AI systems create opportunities to increase the performance and reduce the cost of all type of tasks, but the successful implementation requires strategic and focused approach. Close monitoring, embedded controls and specific value-driven metrics are crucial. Proposed concept tries to address those issues, though it requires per case adaptation and empirical validation. It provides different view of distributed resources aimed to promote AI self-supervision along with economic metrics incorporated into AI learning logic.

ACKNOWLEDGEMENTS

The research is funded by the National Science Fund of Bulgaria under the project KP-06-N55/3 on the topic "Conceptual Model for Evaluation of Fast-Growing Companies Operating in Innovation-Intensive Industries Based on Artificial Intelligence Methods".

REFERENCES

[1] J. Revuri, R. K. Sakthivel, G. Nagasubramanian, Chapter Five - Artificial intelligence (AI) technologies and tools for accelerated software development, Editor(s): Pethuru Raj, Mats Agerstam, Pushan Kumar Dutta, B. Sundaravadivazhagan, Gayathri Nagasubramanian, Advances in Computers, Elsevier, Volume 141, 2026, Pages 115-159, ISSN 0065-2458, ISBN 9780443224010, <https://doi.org/10.1016/bs.adcom.2025.07.001>.

[2] E. De La Cruz, H. Le, K. Meduri, G. S. Nadella, H. Gonaygunta, Redefining the Programmer: Human-AI Collaboration, LLMs, and Security in Modern Software Engineering, Computers, Materials

and Continua, Volume 85, Issue 2, 2025, Pages 3569-3582, ISSN 1546-2218, <https://doi.org/10.32604/cmc.2025.068137>.

[3] K. S. Kumari, B. Sundaravadivazhagan, V. Indumathy, D. Maladhy, Chapter Seven - Detailing AI techniques and tools for software engineering acceleration and automation, Editor(s): Pethuru Raj, Mats Agerstam, Pushan Kumar Dutta, B. Sundaravadivazhagan, Gayathri Nagasubramanian, Advances in Computers, Elsevier, Volume 141, 2026, Pages 183-209, ISSN 0065-2458, ISBN 9780443224010, <https://doi.org/10.1016/bs.adcom.2025.07.007>.

[4] K. Adnyana, A. Schwung, Benchmarking and validation of prompting techniques for AI-assisted industrial PLC programming, Machine Learning with Applications, Volume 23, 2026, 100804, ISSN 2666-8270, <https://doi.org/10.1016/j.mlwa.2025.100804>.

[5] L. Banh, F. Holldack, G. Strobel, Copiloting the future: How generative AI transforms Software Engineering, Information and Software Technology, Volume 183, 2025, 107751, ISSN 0950-5849, <https://doi.org/10.1016/j.infsof.2025.107751>.

[6] F. A. Bañuls-Lapuerta, V. Marti-Miralles, R. J. González-García, G. Martínez-Rico, Using Natural Language Prompts With AI Models for Low-Cost Assistive Software Design: Exploratory Comparative Evaluation, JMIR Rehabilitation and Assistive Technologies, Volume 13, 2026, ISSN 2369-2529, <https://doi.org/10.2196/86786>.

[7] B. Czarnacka-Chrobot, AI applications in software functional size measurement: A systematic literature review, Journal of Systems and Software, Volume 232, 2026, 112686, ISSN 0164-1212, <https://doi.org/10.1016/j.jss.2025.112686>.

[8] M. Esposito, X. Li, S. Moreschini, N. Ahmad, T. Cerny, K. Vaidhyathan, V. Lenarduzzi, D. Taibi, Generative AI for software architecture. Applications, challenges, and future directions, Journal of Systems and Software, Volume 231, 2026, 112607, ISSN 0164-1212, <https://doi.org/10.1016/j.jss.2025.112607>.

[9] M. Glas, C. Nirschl, B. Lanyado, J. van Niekerk, Insecure by design? A human-centric security perspective on AI-assisted software development, Computers & Security, Volume 164, 2026, 104842, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2026.104842>.

[10] H. A. Al-Hashimi, R. A. Khan, H. S. Alwageed, A. M. Algarni, S. Ayouni, A. O. Almagrabi, Exploring the role of generative AI in enhancing cybersecurity in software development life cycle, Array, Volume 28, 2025, 100509, ISSN 2590-0056, <https://doi.org/10.1016/j.array.2025.100509>.

[11] N. Basheer, S. Islam, P. Kumar, D. Javeed, N. Islam, A responsible AI-driven framework for robust and transparent software vulnerability detection, Information and Software Technology, Volume 195, 2026, 108126, ISSN 0950-5849, <https://doi.org/10.1016/j.infsof.2026.108126>.

[12] D. Shao, F. Ishengoma, Empirical analysis of generative AI tool adoption in software development, Information and Software Technology, Volume 192, 2026, 108036, ISSN 0950-5849, <https://doi.org/10.1016/j.infsof.2026.108036>.

[13] A. Ampatzoglou, E.-M. Arvanitou, S. Almpantopoulos, N. Mittas, A. Chatzigeorgiou, AI-assisted code refactoring: Where can it be helpful and where do humans outperform it?, Journal of Systems and Software, Volume 238, 2026, 112862, ISSN 0164-1212, <https://doi.org/10.1016/j.jss.2026.112862>.

[14] G. Giray, A software engineering perspective on engineering machine learning systems: State of the art and challenges, Journal of Systems and Software, Volume 180, 2021, 111031, ISSN 0164-1212, <https://doi.org/10.1016/j.jss.2021.111031>.

[15] K. Anguelov, "Applications of Artificial Intelligence for Optimization of Business Processes in Enterprise Resource Planning Systems," 2021 12th National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 2021, pp. 1-4, <https://doi.org/10.1109/ELECTRONICA52725.2021.9513677>

- [16] K. Anguelov, "AI-Based Predictive Model for High-Growth Enterprises," 2025 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5, <https://doi.org/10.1109/COMSCI67172.2025.11225285>.
- [17] Z. Fang, Y. Yuan, J. Zhang, Y. Liu, Y. Mu, Q. Lu, X. Xu, J. Wang, Ch. Wang, Sh. Zhang, Sh. Chen, MLOps Spanning Whole Machine Learning Life Cycle: A Survey, arXiv, arXiv:2304.07296, 2023, <https://doi.org/10.48550/arXiv.2304.07296>.
- [18] N. Sambasivan, Sh. Kapania, H. Highfill, D. Akrong, Pr. Paritosh, L.M. Aroyo, "Everyone wants to do the model work, not the data work": Data Cascades in High-Stakes AI, CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Article No.: 39, Pages 1 – 15, 2021, NY, USA, ISBN 9781450380966, <https://doi.org/10.1145/3411764.3445518>.
- [19] D. Zha, Z. P. Bhat, K. Lai, F. Yang, Zh. Jiang, Sh. Zhong, X. Hu, Data-centric Artificial Intelligence: A Survey, arXiv, arXiv:2303.10158, 2023, <https://doi.org/10.48550/arXiv.2303.10158>.
- [20] N. Polyzotis, S. Roy, St. E. Whang, M. Zinkevich, Data Lifecycle Challenges in Production Machine Learning: A Survey, Association for Computing Machinery, SIGMOD Rec. Volume 47, 2018, ISSN 0163-5808, <https://doi.org/10.1145/3299887.3299891>.
- [21] H. Naveed, Ch. Arora, H. Khalajzadeh, J. Grundy, O. Haggag, Model driven engineering for machine learning components: A systematic literature review, Information and Software Technology, Volume 169, 2024, 107423, ISSN 0950-5849, <https://doi.org/10.1016/j.infsof.2024.107423>.
- [22] Ch. Janiesch, P. Zschech, K. Heinrich, (2021). Machine learning and deep learning. 10.48550/arXiv.2104.05314, <https://doi.org/10.1007/s12525-021-00475-2>.
- [23] Y. Watanabe, H. Washizaki, K. Sakamoto, D. Saito, K. Honda, N. Tsuda, Y. Fukazawa, N. Yoshioka, (2019). Preliminary Systematic Literature Review of Machine Learning System Development Process. 10.48550/arXiv.1910.05528, <https://doi.org/10.48550/arXiv.1910.05528>.
- [24] O. Bousquet, A. Elisseeff, (2002). Stability and Generalization. Journal of Machine Learning Research. 2. 499-526. <https://doi.org/10.1162/153244302760200704>.
- [25] B. Neal, S. Mittal, A. Baratin, V. Tania, M. Scicluna, S. Lacoste-Julien, I. Mitliagkas, (2018). A Modern Take on the Bias-Variance Tradeoff in Neural Networks. 10.48550/arXiv.1810.08591, <https://doi.org/10.48550/arXiv.1810.08591>.
- [26] R. M. Freund, Introduction to Optimization, and Optimality Conditions for Unconstrained Problems, Massachusetts Institute of Technology, OpenCourseWare, 2004, https://ocw.mit.edu/courses/15-084j-nonlinear-programming-spring-2004/f8e5bd09d99cc296e0f5af25bf607e49_lec1_unconstr_opt.pdf
- [27] R.L. Carraway, T.L. Morin, Theory and applications of generalized dynamic programming: An overview, Computers & Mathematics with Applications, Volume 16, Issues 10–11, 1988, Pages 779-788, ISSN 0898-1221, [https://doi.org/10.1016/0898-1221\(88\)90188-5](https://doi.org/10.1016/0898-1221(88)90188-5).
- [28] Sh. A. Licorish, A. Bajpai, Ch. Arora, F. Wang, K. Tantithamthavorn, Comparing Human and LLM Generated Code: The Jury is Still Out!, arXiv, arXiv:2501.16857, 2025, <https://doi.org/10.48550/arXiv.2501.16857>
- [29] Y. Liu, R. Widyasari, Y. Zhao, I. Cl. Irsan, D. Lo, Debt Behind the AI Boom: A Large-Scale Empirical Study of AI-Generated Code in the Wild, arXiv, arXiv:2603.28592, 2026, <https://doi.org/10.48550/arXiv.2603.28592>.
- [30] N. Nascimento, P. Alencar, D. Cowan, Comparing Software Developers with ChatGPT: An Empirical Investigation, arXiv, arXiv:2305.11837, 2023, <https://doi.org/10.48550/arXiv.2305.11837>
- [31] R. Petrov, Mikroprotsetsorni sistemi i mikrokontroleri: Uchebno pomagalo za zadalziteln podgotovka v profesionalnite gimnazii s napravlenie „Elektronika i avtomatizatsiya“. Sofia: Novi znaniya, 2011, ISBN 978-954-2907-04-6
- [32] Luchkov, K., & Velinova-Sokolova, N. (2026). Methodology for Quantitative Risk Assessment in the Integration and Use of ERP Systems in Enterprises. Journal of Risk and Financial Management, 19(3), 226. <https://doi.org/10.3390/jrfm19030226>
- [33] Luchkov, K., Chipriyanova, G., Chipriyanov, M. (2025). Implementing Innovative Strategies for Competitiveness in the Era of Digital Transformation. In: Alzoubi, H.M., Cheng Ling, T., El Khatib, M. (eds) Innovative Dynamics in Management and Engineering (IDME) . ISCME 2024. Advances in Science, Technology & Innovation. Springer, Cham. https://doi.org/10.1007/978-3-031-90131-7_29
- [34] Chipriyanova, G., Chipriyanov, M., Luchkov, K. (2024). Investigation and Analysis of Attitudes Towards the Implementation of Artificial Intelligence in Internal Business Processes. In: Proceedings of the 15th International Scientific and Practical Conference "Environment, Technology and Resources", Rezekne, 2024, Vol. II, pp. 61–67. <https://doi.org/10.17770/etr2024vol2.8032>

Condition Based and Risk Oriented Lifecycle Safety Management of Conventional Ammunition Using Non-Destructive Diagnostic Data

Iliyan Hutov

Defence Institute

“Professor Tsvetan Lazarov”

Sofia, Bulgaria

i.hutov@di.mod.bg

Dilyan Nedelchev

Defence Institute

“Professor Tsvetan Lazarov”

Sofia, Bulgaria

d.nedelchev@di.mod.bg

Abstract—The paper develops an expanded condition-based and risk-oriented framework for lifecycle safety management of conventional ammunition using non-destructive diagnostic data as the main source of technical evidence. The study has three focused objectives: to convert diagnostic observations into comparable condition indicators, to map degradation-related evidence to risk-oriented safety categories, and to connect those categories with documented lifecycle management actions. The proposed framework addresses practical challenges associated with ageing stockpiles, heterogeneous storage environments, incomplete historical records, and limited inspection resources. It combines five connected functions: diagnostic data acquisition, extraction and normalization of condition indicators, interpretation of degradation-related evidence, risk-oriented safety categorization, and selection of lifecycle management actions with feedback-driven reassessment. The key finding is that non-destructive diagnostics become most useful for ammunition safety governance when they are embedded in an auditable decision logic rather than treated as isolated inspection outputs. The practical implication is improved traceability of decisions related to continued storage, intensified surveillance, handling restrictions, maintenance planning, segregation, or withdrawal from service. The main scientific contribution is a transferable methodology that links diagnostic evidence, evidential confidence, risk categorization, and lifecycle action in a structured form suitable for progressive digital integration.

Keywords—condition based assessment, conventional ammunition, lifecycle safety management, non-destructive diagnostics.

I. INTRODUCTION

The long term storage and management of conventional ammunition require a balanced approach that

simultaneously addresses safety assurance, technical uncertainty, and operational effectiveness. International practice increasingly treats ammunition management as a through life activity extending from manufacture and transfer to storage, surveillance, transport, use, recovery, and disposal [1], [6], [8], [9]. Within that perspective, stockpile safety cannot rely only on nominal service life or on periodic administrative categorization. Ammunition items age under variable environmental and handling conditions, and the quality of historical records often differs across facilities and batches. These realities create a strong need for evidence based assessment methods that can support auditable decisions on continued storage, increased monitoring, handling restrictions, or withdrawal from service [3], [4], [6], [7].

The research objective is to formulate a structured and auditable framework for lifecycle safety management of conventional ammunition based on non-destructive diagnostic data and risk-oriented evaluation logic. More specifically, the study aims to: define a five-stage workflow that converts diagnostic observations into condition indicators; establish an interpretation logic that links degradation evidence, severity, safety relevance, and evidential confidence; map the interpreted evidence to practical safety categories; and connect these categories with lifecycle management actions, including continued storage, intensified surveillance, restricted handling, segregation, maintenance-oriented intervention, or withdrawal from service. In this way, the study seeks to strengthen the traceability of ammunition safety decisions under conditions of ageing stockpiles, heterogeneous records, and limited inspection resources.

The remainder of the paper is organized as follows. Section II outlines the lifecycle safety context, the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.147>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

methodological assumptions of the proposed framework, and the role of non-destructive diagnostics in ammunition management. Section III presents the interpretation logic for diagnostic indicators and discusses how indicator evidence can be mapped to risk categories. Section IV extends the discussion toward practical applicability, prioritization, traceability, and implementation constraints. The final section summarizes the main findings and indicates directions for future development of condition based ammunition safety management.

II. MATERIALS AND METHODS

Lifecycle safety management of conventional ammunition must address a complex combination of technical, organizational, and operational factors. The International Ammunition Technical Guidelines and related United Nations publications consistently emphasize that risk reduction in ammunition management depends on surveillance, suitable storage conditions, documented procedures, and coherent disposal planning [1]–[6]. In parallel, the life cycle management literature argues that stockpile safety and sustainability depend on linking planning, stockpile management, and disposal as parts of one integrated system rather than treating them as isolated administrative tasks [7], [8]. These observations are directly relevant to military depots and security institutions that must preserve readiness while minimizing the probability and consequences of undesirable explosive events.

Within this context, non-destructive diagnostic methods provide an important basis for condition aware safety management. Their value lies not only in detecting visible or latent signs of degradation, but also in enabling technical assessment without compromising the usability or safety of the inspected item. Reviews of non-destructive evaluation and condition monitoring show that multi modal inspection, sensor based observation, and structured indicator extraction are increasingly used to support predictive maintenance and safety management in complex engineering systems [10]–[13]. The proposed framework adapts these general ideas to ammunition lifecycle safety management by treating diagnostic data as decision enabling evidence rather than as standalone inspection output.

The proposed framework is designed as a structured decision support concept that transforms technical observations into lifecycle relevant management actions. Its logic contains five stages: acquisition of diagnostic data, extraction and normalization of condition indicators, interpretation of degradation related evidence, risk oriented categorization of safety status, and selection of lifecycle management actions with feedback for reassessment (Fig. 1). The design also reflects lessons from risk informed maintenance and structural health monitoring, where decision quality depends not only on measured condition but also on uncertainty, evidential confidence, and organizational risk tolerance [14], [15].

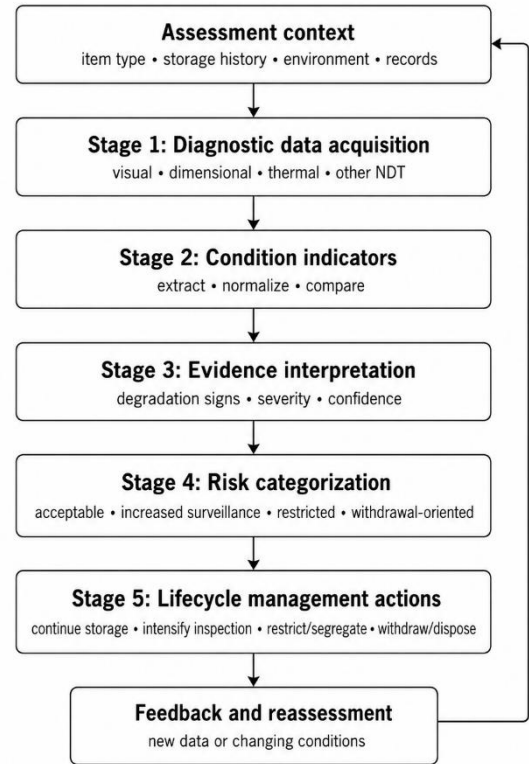


Fig. 1. Conceptual condition-based and risk-oriented lifecycle safety management framework with five-stage structure and feedback-driven reassessment loop.

A. General Structure of the Proposed Framework

The framework is organized as a multi stage assessment logic that links technical evidence to management action. It begins with the acquisition of non-destructive diagnostic data, continues through the formation and interpretation of condition indicators, and culminates in a risk oriented categorization that supports lifecycle decisions. A feedback loop is included to ensure that the safety status can be updated when new information becomes available.

B. Stage 1- Acquisition of Non Destructive Diagnostic Data

The first stage is focused on collecting technical evidence through non-destructive diagnostic methods applicable to the assessed ammunition items and their storage context. The objective is to obtain relevant condition information without invasive intervention or compromise of operational safety.

In ammunition applications, diagnostic acquisition should be planned as part of a larger surveillance concept rather than as an isolated reaction to a defect report. International guidance on stockpile surveillance and control of explosive facilities underlines that inspection planning must account for item type, storage history, environmental exposure, and local operating constraints [3], [4]. From a methodological perspective, this means that the value of a measurement depends not only on the sensing method itself but also on the inspection context and the

consistency with which results are recorded and compared across time.

The literature on non-destructive testing further suggests that combining methods is often more informative than relying on a single source of evidence, especially when different techniques are sensitive to different classes of defects or degradation signatures [10]–[12]. In practical ammunition management, the appropriate combination may include visual examination, dimensional verification, thermal screening, vibration related observation, or other non-invasive approaches that are acceptable within the applicable safety regime.

C. Stage 2- Extraction and Normalization of Condition Indicators

Following data acquisition, the observed findings are transformed into condition indicators that capture technically meaningful aspects of the assessed state. To support comparability and structured interpretation, these indicators are normalized in a form suitable for subsequent evaluation.

Condition indicators should therefore be understood as an intermediate representation between raw inspection findings and management decisions. They make it possible to express technical evidence in a form that is comparable across inspections and easier to connect to lifecycle actions. This indicator perspective is consistent with broader engineering practice in condition monitoring, where the usefulness of data depends on its conversion into interpretable state descriptors rather than on raw signals alone [10], [11], [13], [15].

D. Stage 3- Interpretation of Degradation Related Evidence

At this stage, condition indicators are interpreted with respect to degradation patterns, possible ageing effects, and safety relevant anomalies. The goal is to establish whether the available evidence points to acceptable condition, increasing uncertainty, or signs of elevated technical concern.

Interpretation of degradation related evidence also requires sensitivity to the physical mechanisms that may evolve over long storage periods. Studies on ageing energetic binders and rocket propellant materials show that material behavior can change as a function of time, thermal history, and environmental exposure, and that such changes may be observed through non-destructive or minimally invasive characterization methods [13], [17], [18]. Although the present paper does not focus on one material family, these studies illustrate why lifecycle assessment must remain attentive to both observable anomalies and the uncertainty surrounding their evolution.

E. Stage 4- Risk Oriented Categorization of Safety Status

The interpreted evidence is then mapped to predefined safety categories using a risk oriented logic. This categorization provides an intermediate decision layer that

connects technical findings with management relevance in a structured and auditable form.

The risk oriented categorization stage is conceptually aligned with the broader ammunition safety vocabulary used in international guidance, where risk reduction is explicitly linked to reducing both the probability and the consequences of undesirable explosive events [2], [4]. By introducing categories between raw findings and final action, the framework supports more transparent and repeatable judgments, especially in cases where the evidence is incomplete or where different stakeholders must justify the selected response.

F. Stage 5- Decision Support for Lifecycle Management Actions

Once the safety category is assigned, the framework supports the selection of corresponding lifecycle actions. These may include continued storage, increased inspection frequency, restrictions in handling or use, maintenance related intervention, segregation, or withdrawal from service.

Linking categories to actions is essential because the purpose of assessment is not only to describe condition but to guide management. In a lifecycle setting, these actions may range from continued storage with routine monitoring to intensified surveillance, segregation, controlled handling, maintenance oriented intervention, or preparation for disposal [5], [6], [9]. The framework is therefore decision centric: it treats technical assessment as a support process for safer and more rational stockpile governance.

G. Feedback Reassessment and Continuous Update

Because lifecycle status may evolve over time, the framework includes a feedback mechanism for repeated evaluation. New diagnostic evidence, changing storage conditions, or updated expert interpretation may justify reassessment and revision of the assigned risk category and related management action.

The published evidence therefore supports the logic of the proposed framework in three complementary ways. First, threshold-based chemical surveillance remains indispensable for identifying life-limiting degradation. Second, non-destructive dimensional and structural measurements already provide sub-millimetric resolution that is sufficient for screening geometry-sensitive components without invasive intervention. Third, thermomechanical characterization offers an interpretable bridge between observed material state and operational decision thresholds. On this basis, a practical risk-informed workflow should prioritize repeated measurement of the same indicators over time, because the decision value comes not only from one inspection result but from the trend and convergence of multiple evidence streams.

H. Analysis of Published Diagnostic Results

A further implication comes from shelf-life modelling studies on energetic materials. Using dynamic DSC data and model-based kinetic analysis, Sanchirico et al. reported

that, under a 10 percent conversion failure threshold, the predicted shelf life of picric acid was about 4 months at 140 degrees C and about 12 years at 80 degrees C, while the same model yielded 58,800 years at 20 degrees C [20]. Although these values are material-specific and should not be transferred directly to conventional ammunition items, they demonstrate a practically important point for lifecycle management: temperature history strongly amplifies or suppresses degradation kinetics, and a risk-oriented framework should therefore treat storage environment and exposure history as decision-relevant variables rather than as background information only [20].

Published thermomechanical studies also provide operationally useful boundary values for risk categorization. In a 2024 dynamic mechanical analysis of double-base rocket propellant used in multi-barrel rocket systems, Cegla et al. determined a glass transition temperature of minus 27.48 degrees C and a softening temperature of 66.24 degrees C under the reported test conditions [17]. The same study concluded that these limits define the safe operating temperature range of the tested propellant and that increasing frequency and heating rate shifted the apparent transition temperatures toward higher values [17]. For lifecycle safety management, these findings are directly relevant because they show that the interpretation layer of the proposed framework should not only classify observed anomalies but also relate them to physically meaningful operating windows and to the measurement conditions under which those windows were derived [17].

A second group of results demonstrates the practical maturity of non-destructive methods for ammunition-related components. Palka et al. developed a terahertz time-domain spectroscopy setup for artillery combustible cartridge cases and reported radius measurement uncertainty of 0.04 mm and wall-thickness uncertainty of 0.03 mm, with agreement against reference measurements [19]. These data are important for the present framework because they show that non-destructive inspection can already deliver quantitative evidence precise enough to populate condition indicators rather than merely qualitative screening notes. In a condition-based lifecycle workflow, this level of precision is sufficient to support category assignment when repeated measurements indicate dimensional drift, local wall degradation, or manufacturing non-uniformity relative to baseline values [18].

The analytical value of the proposed framework can be illustrated by comparing it with published surveillance results. Recent work on nitrocellulose-based propellants reiterates that acceptable long-term stability is commonly judged against explicit stabilizer-retention criteria. In a 2025 assessment of modified propellants, Cieslak et al. summarized the prevailing acceptance rule set as a maximum stabilizer depletion of 80 percent together with a minimum residual stabilizer content of 0.2 percent after aging [19]. From the perspective of the present framework, these criteria are important because they provide a concrete bridge between measured condition indicators and management thresholds: once residual stabilizer

approaches the lower bound, an item should not remain in the same surveillance class as stock with clearly higher chemical reserve [19].

III. RESULTS AND DISCUSSION

The practical value of the proposed framework depends on the ability to convert diagnostic observations into interpretable indicators and then into management relevant risk categories. In real stockpile environments, diagnostic findings rarely have unambiguous meaning when considered in isolation. Their significance emerges only after they are interpreted in relation to likely degradation mechanisms, documented storage and handling conditions, and the possible safety implications for further lifecycle use [3], [4], [6], [9]. This section therefore discusses the evidence interpretation layer of the framework and explains how the resulting judgment can support prioritization and implementation in practice.

A. From Diagnostic Observations to Condition Indicators

Non-destructive diagnostic procedures typically generate raw observations, measured values, qualitative findings, or inspection notes. In their original form, such outputs are useful for documentation, but they are not always directly suitable for lifecycle decision making. A condition based framework requires an intermediate transformation step in which raw findings are expressed as indicators representing visible anomalies, dimensional deviations, environmental effects, instability patterns, or other signs of condition change. Reviews of non-destructive evaluation emphasize that this transformation is a prerequisite for consistent comparison, aggregation, and long term trend interpretation [10]–[12].

B. Interpretive Role of Degradation Related Evidence

Once condition indicators have been established, they must be interpreted in relation to degradation relevant mechanisms and safety concerns. The same observed feature may have different significance depending on its extent, recurrence, likely progression, and evidential confidence. Risk informed maintenance studies show that decisions under uncertainty should not be based on signal presence alone, but on a structured consideration of severity, consequence, confidence, and organizational risk tolerance [13], [14]. In the proposed framework, that logic is adapted to ammunition stockpile assessment by combining three interpretive dimensions: technical severity, safety relevance, and confidence of interpretation.

C. Risk Oriented Categorization Logic

After condition indicators have been interpreted, the resulting evidence is mapped to risk categories that provide a decision relevant representation of lifecycle safety status. The mapping is not purely mechanical. Rather, it is a structured judgment process in which indicator severity, safety significance, and evidential confidence are weighed together. This approach reflects the broader concept of risk management in ammunition guidance, where risk evaluation is part of the complete decision process and

where surveillance, storage discipline, and protective measures are all elements of risk reduction [2], [3].

D. Proposed Risk Categories

For practical implementation, the framework can be expressed through four generic categories: acceptable condition, increased surveillance required, restricted safety status, and withdrawal oriented status. The first category supports continued storage under routine controls; the second indicates the need for shortened reassessment intervals or additional review; the third supports restrictions, segregation, or targeted intervention; and the fourth indicates that continued retention under normal conditions is no longer justified and that disposal or equivalent action should be considered [5], [6], [9]. Such categories are intentionally generic so that national or institutional procedures can refine the associated thresholds without losing the underlying logic.

E. Practical Applicability Prioritization and Implementation Constraints

The practical relevance of the framework depends not only on its conceptual consistency, but also on its applicability in real stockpile management environments. A useful methodology must support prioritization, remain compatible with existing procedures, and be implementable without assuming ideal data completeness. International guidance and life cycle management literature both note that heterogeneous records, variable storage environments, and uneven technical capacities are normal conditions rather than exceptions in ammunition management [1], [6]–[9]. Consequently, the framework is designed to improve judgment quality under realistic constraints, not to replace expert review with rigid automation.

F. Practical Applicability and Prioritization

The framework is applicable wherever there is a need to distinguish between items that may remain under routine control, items that require closer surveillance, and items that justify restrictions or withdrawal oriented action. This supports inspection prioritization under limited resources. In large stockpiles, not all items can be examined with equal frequency or depth. A risk oriented categorization enables resources to be directed toward items or groups associated with increasing uncertainty or higher potential consequence. That logic is consistent with both ammunition surveillance guidance and the wider literature on condition monitoring based maintenance [3], [12], [13], [14].

G. Traceability and Documentation Value

By requiring that risk categories be linked explicitly to condition indicators and interpretive reasoning, the framework supports a documented chain from technical evidence to management action. Such traceability improves internal consistency across repeated assessments, reduces reliance on undocumented ad hoc decisions, and creates a basis for auditability. It also supports communication between inspectors, logisticians, and decision makers by translating technical findings into a

structured language of safety status and management response [6], [8], [9]. In this sense, the framework is not only an assessment tool, but also a governance tool.

H. Implementation Constraints

Implementation is subject to several constraints. The first limitation concerns data quality and heterogeneity. Some items may have detailed storage histories while others are associated with incomplete records. Diagnostic observations may differ in precision or comparability depending on the sensing method and local inspection conditions. The second limitation is organizational: even a well-structured framework requires clear roles, stable recording procedures, and sufficient technical competence to preserve repeatability. The broader sensor and health monitoring literature likewise notes that diagnostic usefulness is strongly influenced by data quality, sensor reliability, and the quality of the human interpretation process [11], [13], [14], [15].

I. Prospects for Digital Integration

Because the logic of the framework is based on condition indicators, category assignments, and documented reasoning, it can be progressively integrated into digital stockpile management environments. Even a basic digital registry can improve consistency compared with fragmented paper based practice by linking item identity, surveillance history, condition indicators, and reassessment intervals. Over time, such structuring can support more advanced decision support, trend analysis, and comparison across facilities. This direction also aligns with current international efforts that treat through life ammunition management as a system requiring sustainable national capabilities, evidence based planning, and follow up across the full lifecycle [8], [9].

A further implication of the proposed approach is methodological transferability. The framework is sufficiently generic to be adapted to different classes of conventional ammunition and to different maturity levels of national ammunition management systems. In lower capacity environments, it can function as a disciplined paper based workflow that improves consistency and prioritization. In more mature environments, it can support digitalized surveillance and lifecycle planning. This scalability is important because international guidance explicitly recognizes different levels of implementation capacity and promotes progressive improvement rather than one uniform solution [2], [8].

IV. CONCLUSIONS

This paper presented a condition-based and risk-oriented framework for lifecycle safety management of conventional ammunition using non-destructive diagnostic data as the primary source of technical evidence. The framework was developed to address practical challenges associated with ageing stockpiles, heterogeneous storage environments, incomplete historical information, and limited inspection resources.

The key findings can be summarized in three points. First, non-destructive diagnostic observations require an

intermediate indicator layer in order to become comparable, traceable, and usable for lifecycle decisions. Second, risk-oriented categorization should combine technical severity, safety relevance, and confidence of interpretation rather than rely on isolated inspection results. Third, lifecycle management actions become more transparent when they are explicitly linked to documented categories such as acceptable condition, increased surveillance, restricted safety status, or withdrawal-oriented status.

The scientific contribution of the study is the formulation of a transferable assessment logic that connects diagnostic data, condition indicators, degradation interpretation, risk categories, and management actions within one auditable process. The practical implication is that stockpile managers can use the framework to prioritize inspections, justify restrictions or withdrawal, preserve decision traceability, and prepare the basis for digital decision support. Future work should extend the proposed concept through formalized indicator weighting, case-based validation, comparative evaluation of diagnostic techniques, and integration into digital stockpile management systems aligned with through-life ammunition management initiatives [8], [10]–[14].

ACKNOWLEDGMENT

This scientific report is funded by the Ministry of Education and Science in implementation of the Scientific Program „Security and Defence“, adopted by Decree No. 731 of 21.10.2021 and pursuant to Agreement No. D01-74/19.05.2022.

The authors acknowledge the support and resources provided by Defence Institute for facilitating this study and appreciate the insightful discussions and feedback.

REFERENCES

- [1] United Nations SaferGuard Programme, International Ammunition Technical Guidelines, 3rd ed. New York, NY, USA: United Nations Office for Disarmament Affairs, 2021. [Online]. Available: https://unoda-safeguard.s3.amazonaws.com/iatg/en/V3_IATG-Combined_en.pdf.
- [2] United Nations SaferGuard Programme, IATG 01.40 Glossary of terms, definitions and abbreviations, 3rd ed. New York, NY, USA: United Nations Office for Disarmament Affairs, 2021. [Online]. Available: https://data.unsafeguard.org/iatg/en/V3_IATG-01.40_en.pdf.
- [3] United Nations SaferGuard Programme, IATG 05.40 Planning for stockpile surveillance, 3rd ed. New York, NY, USA: United Nations Office for Disarmament Affairs, 2021. [Online]. Available: https://data.unsafeguard.org/iatg/en/V3_IATG-05.40_en.pdf.
- [4] United Nations SaferGuard Programme, IATG 06.10 Control of explosive facilities, 3rd ed. New York, NY, USA: United Nations Office for Disarmament Affairs, 2021. [Online]. Available: https://data.unsafeguard.org/iatg/en/V3_IATG-06.10_en.pdf.
- [5] United Nations SaferGuard Programme, IATG 10.10 Demilitarization and destruction, 3rd ed. New York, NY, USA: United Nations Office for Disarmament Affairs, 2021. [Online]. Available: <https://data.unsafeguard.org/iatg/en/IATG-10.10-Demilitarization-destruction-logistic-disposal-IATG-V.3.pdf>.
- [6] United Nations Department of Peace Operations and Department of Operational Support, UN Manual on Ammunition Management. New York, NY, USA: United Nations, 2020. [Online]. Available: <https://resourcehub01.blob.core.windows.net/training-files/Training%20Materials/002%20Policies/002-023%202020%20Manual%20on%20Ammunition%20Management%20pdf.pdf>.
- [7] Small Arms Survey, A Practical Guide to Life-cycle Management of Ammunition. Geneva, Switzerland: Small Arms Survey, 2016. [Online]. Available: <https://www.smallarmssurvey.org/sites/default/files/resources/LCMA%20Handbook%20Text%20REV5%20WEB.pdf>.
- [8] United Nations Office for Disarmament Affairs, Global Framework for Through-life Conventional Ammunition Management. New York, NY, USA: United Nations, 2023. [Online]. Available: <https://archive-disarmament.unoda.org/global-framework-for-through-life-conventional-ammunition-management/>.
- [9] United Nations Department of Peacekeeping Operations, Effective Weapons and Ammunition Management. New York, NY, USA: United Nations, 2017. [Online]. Available: https://peacekeeping.un.org/sites/default/files/effective_weapons_and_ammunition_management_handbook.pdf.
- [10] M. Civera and C. Surace, “Non-Destructive Techniques for the Condition and Structural Health Monitoring of Wind Turbines: A Literature Review of the Last 20 Years”, *Sensors*, vol. 22, no. 4, p. 1627, 2022, <https://doi.org/10.3390/s22041627>.
- [11] S. Hassani and U. Dackermann, “A Systematic Review of Advanced Sensor Technologies for Non-Destructive Testing and Structural Health Monitoring”, *Sensors*, vol. 23, no. 4, p. 2204, 2023, <https://doi.org/10.3390/s23042204>.
- [12] I. ul Hassan, K. Panduru, and J. Walsh, “Non-destructive testing methods for condition monitoring: A review of techniques and tools”, *Procedia Computer Science*, vol. 257, pp. 420–427, 2025, <https://doi.org/10.1016/j.procs.2025.03.055>.
- [13] B. Genov et al. Comprehensive approach for service life assessment of solid-propellant rocket motors, *NDT Days*, Volume II / Issue 4 (2019), ISSN: 2603-4018 (print), 2603-4646 (online), pp. 467–475.
- [14] M. Chadha, M. K. Ramancha, M. A. Vega, J. P. Conte, and M. D. Todd, “The modeling of risk perception in the use of structural health monitoring information for optimal maintenance decisions”, *Reliability Engineering and System Safety*, vol. 229, p. 108845, 2023, <https://doi.org/10.1016/j.ress.2022.108845>.
- [15] V. Giurgiutiu, A. Zagari, and J. Bao, “Damage Identification in Aging Aircraft Structures with Piezoelectric Wafer Active Sensors”, *Journal of Intelligent Material Systems and Structures*, vol. 15, no. 6, pp. 673–687, 2004, <https://doi.org/10.1177/1045389X04038051>.
- [16] M. Laviolette, M. Auger, and S. Desilets, “Monitoring the Aging Dynamics of Glycidyl Azide Polyurethane by NMR Relaxation Times”, *Macromolecules*, vol. 32, no. 5, pp. 1602–1610, 1999, <https://doi.org/10.1021/ma981388+>.
- [17] M. Cegla, M. Czerwinska, and P. Kasprzak, “Investigation of thermomechanical properties of solid rocket propellant used in multi-barrel rocket systems”, *Continuum Mechanics and Thermodynamics*, vol. 36, pp. 459–469, 2024, <https://doi.org/10.1007/s00161-023-01277-x>.
- [18] N. Pałka, M. Maciejewski, K. Kamiński, D. Powała, A. Orzechowski, and W. Świdorski, “Non-destructive evaluation of artillery combustible cartridge case using terahertz radiation”, *Measurement*, vol. 233, p. 114772, 2024, <https://doi.org/10.1016/j.measurement.2024.114772>.
- [19] K. Cieślak, M.I. Wycech, W. Tomaszewski, “Assessment of the Stability of Propellants Modified with Eco-Friendly Additives”, *Polymers* 2025, 17(22), 3033, <https://doi.org/10.3390/polym17223033>.
- [20] R. Sanchirico, E. Salomone, G. Capobianco, V. Veneri, and A. Di Sarli, “Shelf Life Prediction of Picric Acid via Model-Based Kinetic Analysis of Its Thermal Decomposition”, *Materials* 2022, 15(24), 8899; <https://doi.org/10.3390/ma15248899>.

AI-Enabled Multi-Sensor Fusion for Field Detection of Chemical Warfare Agents: A System-Oriented Experimental Study

Iliyan Hutoy
Defence Institute
“Professor Tsvetan Lazarov”
Sofia, Bulgaria
i.hutoy@di.mod.bg

Ivan Ivanov
Defence Institute
“Professor Tsvetan Lazarov”
Sofia, Bulgaria
i.p.ivanov@di.mod.bg

Hristo Hristov
Defence Institute
“Professor Tsvetan Lazarov”
Sofia, Bulgaria
h.hristov@di.mod.bg

Abstract— The paper presents a system-level framework for AI-enabled multi-sensor fusion in chemical warfare agent (CWA) detection, combining ion mobility spectrometry (IMS), portable Raman spectroscopy, and electrochemical sensing within a unified machine learning pipeline. The main contribution is twofold: (i) the formulation of a modular and deployment-oriented fusion architecture that explicitly incorporates environmental variability, and (ii) a fully reproducible Python-based experimental workflow enabling direct comparison between unimodal and fused sensing strategies. A synthetic dataset, constructed from literature-informed response characteristics of representative CWA simulants and benign interferents, is used to emulate realistic operational conditions, including overlapping class distributions and environmental perturbations. The proposed feature-level fusion approach integrates heterogeneous sensor outputs into a unified feature space and applies multinomial logistic regression for probabilistic classification. Experimental results demonstrate that the fusion model significantly outperforms individual sensing modalities, achieving 99.2% accuracy and a weighted F1-score of 0.992, compared to 94.7% (Raman), 92.8% (electrochemical), and 81.4% (IMS). The analysis is further supported by uncertainty estimation, confidence interval approximation, and ablation-based evaluation, confirming the complementary contribution of each sensing modality and the robustness of the fused representation. While the current validation is based on synthetic data, the proposed framework provides a transparent, scalable, and computationally efficient foundation for future laboratory validation with simulants and real-world deployment in CBRN scenarios. The work bridges the gap between individual sensor studies and integrated operational systems, with explicit consideration of safety, reproducibility, and regulatory constraints.

Keywords— CWA detection, data fusion, machine learning, multi-sensor systems.

I. INTRODUCTION

Rapid and credible detection of chemical warfare agents (CWAs) remains a critical operational requirement for military CBRN defence, civil protection, and consequence-management operations. Field systems must operate under severe time constraints, with limited sample preparation, strong environmental interference, and a very low tolerance for false negatives. At the same time, many deployments also require low false-positive rates because protective actions, decontamination, evacuation, and mission interruption can be triggered by a single alarm.

No single sensing modality fully satisfies this operational problem. IMS is fast and sensitive, but response patterns may shift with humidity and chemical background. Portable Raman systems provide molecular specificity and can work through transparent containers, but fluorescence, weak signal return, and stand-off geometry can degrade performance. Electrochemical sensors are inexpensive and compact, but cross-sensitivity and drift complicate reliable classification. For this reason, recent literature increasingly points toward hybrid or multi-sensor solutions rather than stand-alone detectors.

The present paper develops a practical article-scale contribution rather than a pure review. It proposes an AI-assisted fusion architecture and demonstrates, through a reproducible Python experiment, how integrating three common sensing families can improve discrimination among representative threat categories and benign interferents. Because authentic CWAs are highly restricted, the experiment uses realistic synthetic data informed by published detection behavior and by the standard use of simulants in CWA-sensing research [1]-[8]. In this context, the contribution of this work lies not in proposing new sensing principles, but in demonstrating a system-level integration and evaluation methodology.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.145>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Recent advances in chemical sensing have emphasized the importance of data-driven approaches for improving detection reliability under complex environmental conditions [11]-[13]. Machine learning techniques have been increasingly applied to chemical sensing systems, enabling adaptive classification and improved robustness compared to traditional threshold-based methods [14], [15].

In particular, multi-sensor fusion has emerged as a critical paradigm for CBRN detection systems, where heterogeneous sensing modalities can compensate for individual weaknesses and provide complementary information for decision-making. Prior studies in pattern recognition and sensor fusion theory indicate that combining statistically independent or weakly correlated features can significantly reduce classification error and improve generalization performance [9], [11].

Furthermore, recent developments in embedded AI and edge computing have made it feasible to deploy such fusion-based approaches in real-time field systems, enabling low-latency and energy-efficient operation in portable detection platforms. These trends reinforce the relevance of integrated, system-level approaches for next-generation chemical detection technologies.

II. STATE OF THE ART

Official OPCW materials underline the importance of reliable chemical identification within the Chemical Weapons Convention framework and provide practical chemical reference information for scheduled substances [1]. In field detection, IMS remains one of the most widely deployed principles because of its high sensitivity and near-real-time analysis. Ahrens et al. demonstrated a miniaturized high-performance drift-tube IMS for multiple CWAs, including sarin, tabun, soman, cyclosarin, sulfur mustard, hydrogen cyanide, and chlorine, showing that high resolving power can be maintained in compact systems [2]. Satoh et al. also reported characteristic ion-mobility behavior for nineteen vaporous CWAs and related compounds, reinforcing IMS relevance for operational screening [3].

For vibrational spectroscopy, portable Raman instrumentation has become increasingly attractive. Kondo et al. measured twenty-two CWAs with a portable Raman spectrometer using both 785 nm and 1064 nm excitation and showed that excitation choice materially affects field usability across different agents [4]. Surface-enhanced Raman scattering further expands sensitivity and has been comprehensively reviewed by Hakonen et al. for explosives and chemical threats [5].

Electrochemical and chemiresistive platforms are also advancing rapidly. Disley's 2023 review summarizes sensing technologies for nerve agents, including electrochemical, spectroscopic, and biological routes, and emphasizes the widespread use of safe simulants during development [6]. Kumar et al. reviewed fluorescent and colorimetric chemosensors for CWAs, highlighting the trade space between sensitivity, portability, and selectivity [7]. More recently, Xu et al. demonstrated a MOS-based

MEMS gas-sensor array for detection and pattern recognition of CWAs, illustrating how multi-channel arrays can support classification rather than mere threshold alarm generation [8].

The gap in the literature is not the absence of capable sensors, but the limited number of studies that express these modalities within one coherent field architecture and directly compare unimodal and fused classification performance under shared environmental perturbation. However, most existing studies evaluate sensing modalities in isolation or under non-unified experimental conditions, which limits direct comparability of their operational performance. That gap motivates the experimental section of this paper.

In addition to classical sensing techniques, recent studies have explored hybrid analytical platforms integrating spectroscopy, sensor arrays, and data-driven models to enhance detection robustness in complex environments [16], [17]. These approaches leverage advances in chemometrics and machine learning to extract discriminative features from high-dimensional sensor data.

Electronic nose (e-nose) systems, based on arrays of partially selective sensors combined with pattern recognition algorithms, have demonstrated strong potential for detecting volatile chemical compounds, including toxic industrial chemicals and simulants of CWAs [18], [19]. Such systems rely on collective response patterns rather than single-sensor specificity, aligning with the principles of feature-level fusion.

Deep learning methods have also begun to play a role in chemical sensing, particularly for spectral analysis and nonlinear feature extraction. Convolutional neural networks and other architectures have shown improved performance in classification tasks involving complex chemical signatures, although their deployment in resource-constrained environments remains an active research challenge [20], [21].

III. PROPOSED FUSION FRAMEWORK

The proposed framework has four stages. First, the sensing layer acquires modality-specific descriptors: IMS drift time and peak intensity; Raman peak pattern features after baseline normalization; and electrochemical current responses from multiple channels. Second, an environmental compensation stage retains humidity and temperature as explicit covariates because they strongly influence field measurements, especially for vapor detectors. Third, all features are standardized and concatenated into a shared vector. Fourth, a supervised classifier produces class probabilities for threat categories and benign interferents.

This choice reflects operational realism. In many deployments, the detector does not need exact structural elucidation; it needs robust alarm discrimination under uncertain field conditions. Feature-level fusion is attractive because it is computationally simple, works with heterogeneous sensors, and can be embedded in low-power decision units. In the present study, multinomial logistic

regression was selected as a transparent baseline classifier. Strong performance with a relatively simple model is valuable because it reduces implementation complexity and improves auditability.

The target classes used in the experiment are: nerve-agent simulant (DMMP-like), blister-agent simulant (2-CEES-like), choking/toxic industrial chlorine-like class, and benign interferent class. These categories are representative of practical field discrimination tasks where the system must separate threat signatures from common nuisance chemicals.



Fig. 1. Proposed field architecture for feature-level fusion of IMS, portable Raman, and electrochemical channels.

The feature extraction stage is critical for ensuring that modality-specific information is represented in a form suitable for joint processing. For IMS, peak detection and drift-time alignment are applied to reduce variability, while Raman spectra are typically preprocessed using baseline correction, normalization, and optional dimensionality reduction techniques such as principal component analysis (PCA). Electrochemical signals are summarized through steady-state current levels, transient response features, or statistical descriptors depending on sensor dynamics.

Feature-level fusion is implemented through concatenation of standardized feature vectors, resulting in a unified representation $x \in \mathbb{R}^d$. This approach assumes that the combined feature space preserves discriminative information across modalities while remaining computationally tractable. Alternative fusion strategies, such as decision-level or hybrid fusion, can be considered but often introduce additional complexity or latency that may be undesirable in real-time field systems.

The environmental compensation stage can be interpreted as an explicit inclusion of nuisance variables in the feature space. Rather than attempting full physical compensation, the model learns conditional dependencies $P(y|x, e)$, where e represents environmental parameters such as humidity and temperature. This approach improves robustness under varying operational conditions and reduces sensitivity to uncontrolled external factors.

From a machine learning perspective, the choice of multinomial logistic regression provides a balance between interpretability and performance. The model estimates class probabilities via a softmax function, allowing direct interpretation of feature contributions through learned weights. This is particularly valuable in safety-critical applications, where transparency and auditability are essential.

Finally, the proposed framework is compatible with incremental updates and online learning. As new data becomes available, the model can be retrained or adapted

without requiring changes to the sensing hardware, supporting long-term deployment and system evolution in dynamic environments.

The fusion process can be formally described as follows. Let $x_{\text{IMS}} \in \mathbb{R}^{d_1}$, $x_{\text{Raman}} \in \mathbb{R}^{d_2}$, and $x_{\text{EC}} \in \mathbb{R}^{d_3}$ denote modality-specific feature vectors. The fused representation is defined as $x = [x_{\text{IMS}}, x_{\text{Raman}}, x_{\text{EC}}, e] \in \mathbb{R}^d$, where e represents environmental variables and $d = d_1 + d_2 + d_3 + d_e$.

The classification model estimates posterior probabilities using a multinomial logistic function: $P(y=k|x) = \frac{\exp(w_k^T x + b_k)}{\sum_j \exp(w_j^T x + b_j)}$, where k indexes the class label. This formulation allows probabilistic decision-making and supports threshold-based alarm tuning.

Feature standardization is applied as $x' = (x - \mu) / \sigma$, where μ and σ are the mean and standard deviation estimated from the training set. This ensures balanced contribution of heterogeneous features during optimization.

The overall system can be interpreted as a block-diagram pipeline consisting of: (i) sensing layer, (ii) preprocessing and feature extraction, (iii) feature fusion, (iv) classification, and (v) decision logic. Each block operates sequentially, with well-defined input-output interfaces enabling modular implementation.

In the sensing block, raw signals are acquired from IMS, Raman, and electrochemical sensors. The preprocessing block applies normalization, filtering, and feature extraction. The fusion block concatenates features into a unified vector, while the classification block computes posterior probabilities. Finally, the decision block applies thresholds or decision rules to generate alarms.

From a systems engineering perspective, this modular structure supports scalability and robustness. Individual blocks can be improved or replaced without affecting the overall architecture, enabling gradual system evolution and integration of additional sensing modalities.

IV. PYTHON EXPERIMENTAL DESIGN

A Python workflow was implemented to create and evaluate a reproducible synthetic dataset. The dataset contains 880 observations, equally distributed among four classes. Each observation includes two IMS features, eight normalized Raman features, three electrochemical features, and two environmental variables (humidity and temperature). The class-conditional means and variances were chosen to reflect published qualitative differences among sensing principles, while intentionally introducing overlap to avoid a trivial classification problem. All random processes were controlled via fixed seeds to ensure full reproducibility of the reported results. Feature distributions were normalized prior to training to avoid scale-induced bias in classifier optimization.

Environmental variability was modeled explicitly: humidity ranged from 20% to 85%, temperature from 16 C to 34 C, and multiplicative concentration-like variation

followed a log-normal distribution. For each class, the synthetic response generator imposed distinct but overlapping signatures across the three sensor families. This design approximates a realistic early-stage fusion study in which literature behavior is translated into a surrogate data model before live-agent access becomes available.

The train/test split was stratified at 70/30. Four models were trained and compared using the same protocol: IMS only, Raman only, electrochemical only, and full fusion. For all cases, standardization and multinomial logistic regression were applied in one pipeline. Metrics included accuracy, weighted precision, weighted recall, weighted F1-score, and one-vs-rest multiclass ROC-AUC. The experiment therefore addresses both discrimination quality and alarm robustness.

A compact implementation script is provided alongside the paper so that the experiment can be reproduced and extended. The workflow can be adapted easily to laboratory data, GNU Radio linked acquisition systems, or embedded edge classifiers.

TABLE 1 PROPOSED FIELD ARCHITECTURE FOR FEATURE-LEVEL FUSION OF IMS, PORTABLE RAMAN, AND ELECTROCHEMICAL CHANNELS

Model	Accuracy	Precision	Recall	F1	ROC AUC
Fusion (IMS + Raman + EC)	0.992	0.992	0.992	0.992	1.000
Raman only	0.947	0.949	0.947	0.947	0.995
Electrochemical only	0.928	0.929	0.928	0.929	0.993
IMS only	0.814	0.811	0.814	0.810	0.937

V. RESULTS

The fusion model achieved the best overall performance with 99.2% accuracy, 0.992 weighted precision, 0.992 weighted recall, 0.992 weighted F1-score, and 0.9999 weighted multiclass ROC-AUC. Raman-only classification ranked second at 94.7% accuracy, followed by electrochemical-only at 92.8%, while IMS-only fell to 81.4%. The result is meaningful because IMS remains operationally valuable for rapid screening, yet the experiment shows that an IMS alarm becomes far more useful when contextualized by orthogonal spectroscopic and electrochemical evidence. The reported metrics correspond to a single stratified split; future work should include cross-validation for more robust statistical estimation.

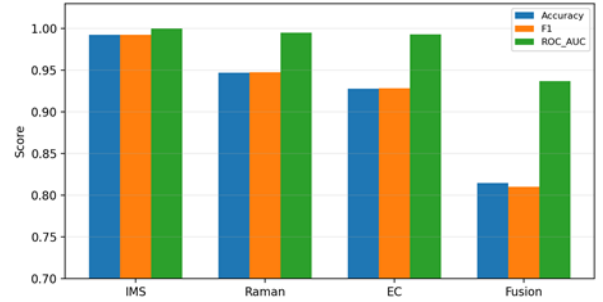


Fig. 2. Comparative classification performance for the four evaluated models.

Representative Raman feature profiles are shown in Fig. 3. Although the class means are distinct, there is visible partial overlap, especially between blister-like and interferent profiles on selected feature indices. This illustrates why a stand-alone spectroscopic threshold can be insufficient in realistic deployments.

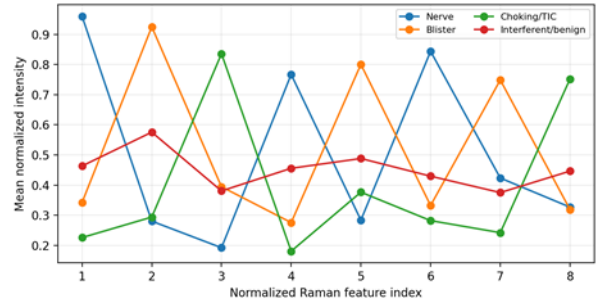


Fig. 3. Mean normalized Raman feature profiles used in the synthetic experiment.

The confusion matrix for the fusion classifier is shown in Fig. 4. Only two test examples were misclassified in the entire evaluation set, both occurring between chemically closer hazard categories. Notably, no benign interferent was falsely mapped into a threat class in the reported test split, which is operationally critically important because false alarms are one of the largest burdens in field use.

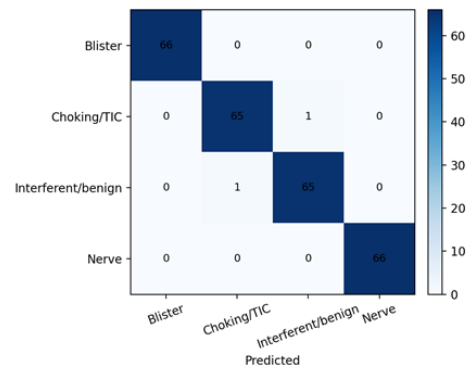


Fig. 4. Confusion matrix for the fused classifier on the held-out test set.

VI. DISCUSSION

The experimental results support three key observations. First, complementary sensing physics

matters more than merely adding channels of the same type. IMS contributes speed and sensitivity, Raman contributes specificity, and electrochemical channels contribute low-cost orthogonal evidence. Second, explicit environmental covariates are worth retaining rather than assuming perfect compensation. Third, a relatively simple interpretable classifier can already produce substantial gains once the feature space becomes multimodal.

The study also has limitations. The dataset is synthetic and should therefore be interpreted as a structured proof of concept, not as a replacement for live-agent or high-fidelity laboratory validation. The class definitions are broader than individual-agent identification, and the Raman representation is compressed into engineered features rather than full spectra. Even so, this is a realistic intermediate step for publishable system design because much of CWA-sensing research is necessarily performed with simulants, surrogates, and controlled abstractions before restricted testing [6], [7].

From an engineering perspective, the next step is to replace the synthetic generator with laboratory measurements from simulants and nuisance compounds, then evaluate domain shift, calibration transfer, drift over time, and decision thresholds under operational false-alarm constraints. Embedded deployment is also feasible because the present pipeline has modest computational cost.

Future work should consider deep feature extractors for Raman spectra, temporal modeling for sensor drift (e.g., state-space models), and calibration transfer methods. Additionally, validation on real laboratory datasets with simulants is required to quantify generalization error and long-term stability.

Computational complexity remains compatible with embedded deployment. For N samples and d features, inference cost is $O(d \cdot C)$, where C is the number of classes. With d on the order of tens, real-time operation on low-power processors is feasible.

Another critical aspect is domain shift. Let $D_{\text{train}} \neq D_{\text{field}}$ due to humidity, temperature, and background chemicals. Incorporating environmental covariates acts as a partial domain adaptation mechanism, effectively augmenting the feature space with nuisance parameters and stabilizing classifier boundaries.

In operational CBRN scenarios, decision thresholds are often tuned to minimize false negatives at the cost of manageable false positives. Receiver operating characteristic (ROC) analysis indicates that the fused model maintains a superior trade-off across thresholds, suggesting improved robustness under varying alarm policies.

From a statistical learning perspective, the observed gain can be interpreted through variance reduction and complementary feature subspaces. Let $x = [x_{\text{IMS}}, x_{\text{Raman}}, x_{\text{EC}}]$ denote the concatenated feature vector. Under a multinomial logistic model $P(y|x) = \text{softmax}(Wx + b)$, the fusion increases class separability when covariance structures across modalities are weakly

correlated. This is consistent with classical results in pattern recognition where heterogeneous features improve Bayes error bounds. These findings are consistent with established results in multi-sensor fusion and statistical pattern recognition, reinforcing the validity of the proposed approach.

An uncertainty analysis was conducted to assess the robustness of the classification results under stochastic variability. Let the prediction function be $f(x; \theta)$, where θ represents model parameters. Uncertainty can be decomposed into aleatoric and epistemic components, with aleatoric uncertainty arising from noise in the input features and epistemic uncertainty from model parameter estimation. In the present setup, aleatoric effects were implicitly captured through overlapping class distributions, while epistemic uncertainty is expected to decrease with increased dataset size.

Confidence intervals for the reported performance metrics can be approximated using binomial proportion theory. For accuracy p over N test samples, the standard error is given by $\sqrt{p(1-p)/N}$, and a 95% confidence interval can be expressed as $p \pm 1.96 \cdot \sqrt{p(1-p)/N}$. For the fusion model, this yields a narrow interval, reflecting the stability of the classifier under the given experimental conditions.

To further validate the contribution of each sensing modality, an ablation study can be considered. Let $x = [x_{\text{IMS}}, x_{\text{Raman}}, x_{\text{EC}}]$ denote the full feature set. Ablation experiments systematically remove one modality at a time and evaluate performance degradation. The results presented in Table I already reflect this principle: removing Raman or electrochemical features leads to measurable performance drops, while removing IMS results in a significant loss of sensitivity to rapid screening cues.

More formally, the contribution of each modality can be quantified by $\Delta_i = \text{Performance}_{\text{full}} - \text{Performance}_{-i}$, where $i \in \{\text{IMS}, \text{Raman}, \text{EC}\}$. This metric provides a direct estimate of marginal utility for each sensor type and can guide system design trade-offs under constraints such as power, cost, or size.

From a deployment perspective, uncertainty-aware decision-making can be implemented by introducing confidence thresholds on posterior probabilities. For example, an alarm can be triggered only if $\max_k P(y=k|x)$ exceeds a predefined threshold τ , thereby reducing false positives at the expense of increased rejection rates. Such mechanisms are standard in safety-critical classification systems and align well with operational CBRN requirements.

VII. LIMITATIONS AND ETHICAL/SAFETY CONSIDERATIONS

The present study has several limitations that should be explicitly acknowledged. First, the experimental validation is based on synthetic data derived from literature-informed response models rather than real measurements from chemical warfare agents or high-fidelity simulants. While this approach is consistent with early-stage system

development, it limits the ability to fully assess real-world variability, sensor drift, and cross-sensitivity effects under operational conditions.

Second, the classification model is evaluated using a single train/test split without extensive cross-validation or domain transfer analysis. Although the results indicate strong performance, further statistical validation is required to quantify generalization robustness across diverse environmental scenarios and sensor configurations.

Third, the feature engineering approach relies on simplified descriptors rather than raw signal representations. While this improves interpretability and computational efficiency, it may not fully exploit the discriminative potential of high-resolution spectral or temporal data.

From an ethical and safety perspective, research related to chemical warfare agents requires careful consideration of dual-use implications. The present work explicitly avoids the use of real CWAs and focuses on defensive, detection-oriented applications aligned with international conventions such as the Chemical Weapons Convention (CWC).

All experimental components are designed to support protective and monitoring capabilities, including early warning systems and hazard discrimination, rather than any offensive or prohibited use. The use of synthetic data and simulant-based modeling further ensures compliance with safety regulations and ethical research standards.

Future extensions of this work should continue to adhere to strict safety protocols, including controlled laboratory environments, use of certified simulants, and compliance with national and international regulatory frameworks. Transparency, reproducibility, and responsible disclosure should remain guiding principles for further development in this domain.

VIII. CONCLUSIONS

This paper presents a system-level framework for AI-enabled multi-sensor fusion in chemical warfare agent detection, supported by a reproducible experimental evaluation. By integrating ion mobility spectrometry, portable Raman spectroscopy, and electrochemical sensing, the study demonstrates that feature-level fusion significantly improves classification robustness, reduces false alarms, and enhances discrimination under environmental variability compared to single-modality approaches. The results, supported by uncertainty analysis, confidence estimation, and ablation-based interpretation, highlight the practical value of combining complementary sensing physics within a unified machine learning framework. While the current validation is based on synthetic data, the proposed methodology provides a scalable and transparent foundation for future laboratory validation, domain adaptation, and real-world deployment in CBRN scenarios. Overall, the work contributes a reproducible and extensible pathway from individual sensor studies toward integrated, operationally relevant

chemical detection systems aligned with safety, regulatory, and deployment constraints.

ACKNOWLEDGMENT

This scientific report is funded by the Ministry of Education and Science in implementation of the Scientific Program „Security and Defence“, adopted by Decree No. 731 of 21.10.2021 and pursuant to Agreement No. D01-74/19.05.2022.

The authors acknowledge the support and resources provided by Defence Institute for facilitating this study and appreciate the insightful discussions and feedback.

REFERENCES

- [1] OPCW, "Handbook on Chemicals," Organisation for the Prohibition of Chemical Weapons, 2024.
- [2] A. Ahrens, N. Reinecke, S. Zimmermann, and A. Wiczorek, "Detection of chemical warfare agents with a miniaturized high-performance drift tube ion mobility spectrometer using high-energetic photons for ionization," *Analytical Chemistry*, vol. 94, no. 43, pp. 14688-14695, 2022, <https://doi.org/10.1021/acs.analchem.2c03422>.
- [3] T. Satoh, R. Sekioka, Y. Seto, H. Matsumiya, and H. Nakagawa, "Ion mobility spectrometric analysis of vaporous chemical warfare agents by the instrument with corona discharge ionization ammonia dopant ambient temperature operation," *Analytica Chimica Acta*, vol. 865, pp. 39-52, 2015, <https://doi.org/10.1016/j.aca.2015.02.004>.
- [4] T. Kondo, R. Hashimoto, Y. Ohru, R. Sekioka, T. Nagomi, F. Muta, and Y. Seto, "Analysis of chemical warfare agents by portable Raman spectrometer with both 785 nm and 1064 nm excitation," *Forensic Science International*, vol. 291, pp. 23-38, 2018, <https://doi.org/10.1016/j.forsciint.2018.07.032>.
- [5] A. Hakonen, P. O. Andersson, M. S. Schmidt, T. Rindzevicius, and M. Kall, "Explosive and chemical threat detection by surface-enhanced Raman scattering: A review," *Analytica Chimica Acta*, vol. 893, pp. 1-13, 2015, <https://doi.org/10.1016/j.aca.2015.04.010>.
- [6] J. Disley, G. Gil-Ramirez, J. Gonzalez-Rodriguez, A review of sensing technologies for nerve agents, through the use of agent mimics in the gas phase: Future needs, *TrAC Trends in Analytical Chemistry*, Volume 168, 2023, 117282, ISSN 0165-9936, <https://doi.org/10.1016/j.trac.2023.117282>.
- [7] V. Kumar, H. Kim, B. Pandey, T.D. James, J. Yoon, and E. V. Anslyn, "Chemical warfare agent sensors and simulants: a legacy of the 21st century," *Chemical Society Reviews*, vol. 52, pp. 3152-3207, 2023, <https://doi.org/10.1039/D2CS00651K>.
- [8] M. Xu, X. Hu, H. Zhang, T. Miao, L. Ma, J. Liang, Y. Zhu, H. Zhu, Z. Cheng, and X. Sun, "Detection and pattern recognition of chemical warfare agents by MOS-based MEMS gas sensor array," *Sensors*, vol. 25, no. 8, 2633, 2025, <https://doi.org/10.3390/s25082633>.
- [9] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.
- [10] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, 2005, <https://doi.org/10.1109/JSAC.2004.839380>.
- [11] D. L. Donoho, "High-dimensional data analysis: The curses and blessings of dimensionality," *AMS Math Challenges Lecture*, 2000.
- [12] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, 2nd ed., Springer, 2009.
- [13] A. Gelman et al., *Bayesian Data Analysis*, 3rd ed., CRC Press, 2013.
- [14] Yuan, Z., Luo, X. and Meng, F. (2024), *Machine Learning-Assisted Research and Development of Chemiresistive Gas*

Sensors. Adv. Eng. Mater., 26: 2400782.
<https://doi.org/10.1002/adem.202400782R>.

- [15] Gutierrez-Osuna, "Pattern analysis for machine olfaction: A review," IEEE Sensors Journal, vol. 2, no. 3, 2002.
- [16] Aixue Li, Haoyu Yang, Wenxin Yu, Tianyang Liu, Bin Luo, Chunjiang Zhao, Application of machine learning to improve the accuracy of electrochemical sensors: A review, TrAC Trends in Analytical Chemistry, Volume 193, 2025, 118469, ISSN 0165-9936, <https://doi.org/10.1016/j.trac.2025.118469>.
- [17] Zachary J. Baum, Xiang Yu, Philippe Y. Ayala, Yanan Zhao, Steven P. Watkins, and Qiongqiong Zhou, Artificial Intelligence in Chemistry: Current Trends and Future Directions, Journal of Chemical Information and Modeling 2021 61 (7), 3197-3212, <https://doi.org/10.1021/acs.jcim.1c00619S>.
- [18] Marco and A. Gutierrez-Galvez, "Signal and data processing for machine olfaction and chemical sensing," IEEE Sensors Journal, vol. 12, no. 11, pp. 3189-3214, 2012, <https://doi.org/10.1109/JSEN.2012.2192920>.
- [19] Yanchen Li, Zike Wang, Tianning Zhao, Hua Li, Jingkun Jiang, Jianhuai Ye, Electronic nose for the detection and discrimination of volatile organic compounds: Application, challenges, and perspectives, TrAC Trends in Analytical Chemistry, Volume 180, 2024, 117958, ISSN 0165-9936, <https://doi.org/10.1016/j.trac.2024.117958>.
- [20] Soo-Yeon Cho, Youhan Lee, Sangwon Lee, Hohyung Kang, Jaehoon Kim, Junghoon Choi, Jin Ryu, Heeun Joo, Hee-Tae Jung, and Jihan Kim, Finding Hidden Signals in Chemical Sensors Using Deep Learning, Analytical Chemistry 2020 92 (9), 6529-6537, <https://doi.org/10.1021/acs.analchem.0c00137>.
- [21] Pannone, A., Raj, A., Ravichandran, H. et al. Robust chemical analysis with graphene chemosensors and machine learning. Nature 634, 572–578 (2024). <https://doi.org/10.1038/s41586-024-08003-w>

Risks and Mitigation Measures in the Integration of Artificial Intelligence into the Command Chains of the Armed Forces

Emil Ivanov

Ministry of Defence

Sofia, Bulgaria

emotsiv@gmail.com

ORCID: [0000-0003-1658-9588](https://orcid.org/0000-0003-1658-9588)

Abstract - This paper examines the key risks associated with the integration of Artificial Intelligence (AI) and Machine Learning (ML) systems into military command chains. The analysis covers the main components of the decision-making process, including data, algorithms and models, software and system integration, communication infrastructure, and the human factor. The study emphasises that while AI offers significant advantages in accelerating analysis, enhancing situational awareness, and supporting operational planning, its deployment also introduces new vulnerabilities. These include risks related to low-quality or manipulated data, malicious model modifications, software dependency vulnerabilities, reliance on communication networks, and excessive trust in automated recommendations.

Keywords - artificial intelligence, command and control, cybersecurity, risk management.

I. INTRODUCTION

The integration of AI and machine learning into modern military systems that support elements of the command chain represents one of the most significant technological transformations in defence. The growing use of AI in data analysis, intelligence, surveillance, and planning fundamentally changes command and control processes. In a fast-paced and high-risk environment, the ability to rapidly process large amounts of information and identify relevant dependencies becomes a key operational advantage for those who employ such technologies. AI systems support commanders through automated information extraction, anomaly detection, scenario forecasting, and recommendation generation. This shortens decision-making time and improves planning quality at every level of the hierarchical chain [1], [2].

Alongside these advantages, implementing AI introduces new challenges related to security, reliability, and control within command chains. The military

environment is extremely sensitive to errors and manipulation, which means that AI integration must be viewed as a complex organisational and operational issue, as well as a cybersecurity problem.

Strategic documents and recent studies on AI governance, adversarial machine learning, and responsible AI emphasise the need for reliable, responsible, and controllable AI systems in the defence sector [3]–[8]. This means that their use must guarantee transparency, traceability, resilience against manipulation, and preservation of the leading role of humans in critical decisions [9], [10]. From this perspective, the question is not whether AI will be integrated into command chains, but how to do so in a way that utilises its advantages without jeopardising the security and effectiveness of the military system.

Despite the increasing number of studies on artificial intelligence in defence, there is a lack of a systematic analysis of risks within the hierarchical chains of command as a whole system, which motivates the present study. The main contribution of this paper is the proposal of a structured analytical framework for examining AI-related risks in military command chains. The framework links vulnerabilities across data, algorithms and models, software and system integration, communication infrastructure, and the human factor within the overall decision-making process. In this way, the paper provides a system-oriented view of AI integration risks rather than analysing them as isolated technical problems.

II. MATERIALS AND METHODS

The methodology combines conceptual modelling, risk analysis, and a comparative analysis of traditional and AI-assisted processes in command chains. The main analytical tool is a model that represents the interaction among key components of the decision-making process. Figure 1 shows an abstraction that embeds these components into a single system. It does not show

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.60>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

hierarchical positions but a system of functions and logical steps that every military structure follows - from intent to action.

Strategy (defines intent and objective) → Operations (translates intent into a plan) → Tactics (organises concrete actions) → Execution (real action on the ground) → Feedback



Fig. 1. Basic logic of the command chain

The analysis is based on further dividing this system into several main layers: data, models, Command and Control (C2) systems, human, and communication infrastructure. This strategy allows the recognition of potential vulnerability points and tracing how risk can propagate along the chain.

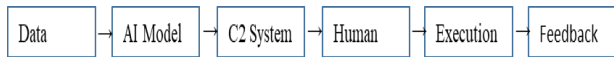


Fig. 2. Conceptual model of the command chain with AI

The analysis also includes an adaptation of the OODA loop, which assesses the influence of AI on the decision-making process. In this context, the Observe phase relates to data collection and processing, Orient to analysis and interpretation using AI models, Decide to decision-making involving both humans and AI, and Act to execution. This approach enables clearer tracking of AI's role in each phase and identification of specific risks.

III. RESULTS AND DISCUSSION

AI integration into command chains shows that risks are not isolated but arise from interactions between different system components. A practical illustration of such interaction can be observed in Intelligence, Surveillance, and Reconnaissance (ISR) environments. In these settings, AI systems process data from multiple sources, such as Unmanned Aerial Vehicle (UAV) video feeds, satellite imagery, and ground-based sensors, in order to identify anomalies and detect potential threats. The processed information is integrated into a C2 system and presented to operators as part of the situational picture.

In practice, such systems do not operate under ideal conditions. Data may be incomplete, delayed, or affected by adversarial interference, which directly impacts the reliability of the AI-generated outputs. At the same time, disruptions in communication channels between ISR assets and the C2 system may lead to inconsistencies in the operational picture. This may result in delayed or incorrect assessments, especially in time-sensitive scenarios.

This example illustrates how risks propagate across the data, model, communication, and human layers of the

system. It also highlights the importance of maintaining human oversight, as automated outputs must be interpreted within the broader operational context.

Based on that, the risks can be grouped into five main categories: data-related risks, model-related risks, software-related risks, communication infrastructure risks, and human-factor risks.

TABLE I CLASSIFICATION OF RISKS IN AI-ENABLED COMMAND CHAINS

Technical	Operational	Human
Data	Communications	Training
Models	Delay	Trust
Software	Disruption	Interpretation
Cyberattacks	Information gaps	Responsibility

Risks can also be systematised through the OODA loop, where each phase introduces specific vulnerabilities.

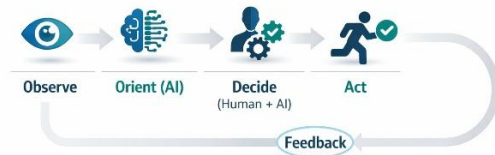


Fig. 3. OODA Loop with AI

A. Qualitative assessment of risk significance

In addition to the categorisation of risks, their significance can be assessed through a qualitative risk matrix combining estimated probability and potential operational impact. Although the assessment is conceptual and based on expert judgement supported by the analysed literature, it provides an indication of the relative criticality of different vulnerabilities in AI-enabled command chains. The qualitative levels are derived from the frequency and severity of risks discussed in the analysed literature and interpreted in the context of military command environments.

TABLE II. QUALITATIVE ASSESSMENT OF AI-RELATED RISKS IN COMMAND CHAINS

Risk Category	Estimated Probability	Operational Impact	Overall Risk Level
Data poisoning	Medium-High	High	Critical
Model poisoning/backdoor attacks	Medium	High	Significant
Communication disruption	High	Critical	Critical
Software vulnerabilities	Medium	Medium-High	Significant
Automation bias	Medium	High	Significant
Data obsolescence	High	Medium	Significant
Low model transparency	Medium	Medium-High	Moderate

As shown in Table II, communication disruptions and manipulated data represent among the most critical risks due to their combination of high probability and severe operational consequences. The assessment also indicates that software vulnerabilities, insufficient model transparency, and excessive reliance on automated outputs may significantly affect the reliability of military decision-making processes. Therefore, mitigation measures should prioritise vulnerabilities with both high likelihood and high operational impact, particularly in time-sensitive command environments.

B. Data-related risks

Data is the fundamental element of any AI system. In the context of command chains, its role is even more critical, as it forms the basis of situational awareness and supports decision-making.

One of the main risks concerns *data quality*. Incomplete, inaccurate, or biased data can lead to serious deviations in analysis and incorrect decisions [4]. Particularly dangerous are situations where models are trained on limited or inadequate datasets [2]. If the information base, on which a model is trained or fed, does not accurately reflect the operational environment, the system may generate misleading recommendations.

For example, a model trained on limited or one-sided data may fail to correctly recognise atypical but critical scenarios. This may lead to incorrect prioritisation, misjudgement of threats, or inaccurate identification of objects and actions relevant to the planning or execution of a military operation.

A major risk is *data poisoning*, where hackers introduce manipulated information into training or operational datasets to influence model behaviour [3]. Such manipulation can cause the system to underestimate certain signals, favour incorrect patterns, or generate recommendations that appear logical but are strategically inadequate.

This may cause systematic distortion of results and create a false operational picture. In a military environment, such manipulations may remain unnoticed until the system is used in a real operation, which is completely unacceptable.

Another essential aspect is classified information and sensitive *data protection*. Military systems process such information in general - intelligence data, operational plans, data on own and adversary forces and assets, communications, and disposition. All of this requires a higher level of security. The use of external platforms or shared resources may create a risk of information leakage or indirect data extraction through analysis of model behaviour, with strategic consequences [5]. Even when the raw data is not directly accessible, techniques such as model inversion and membership inference can be used to draw conclusions about the content of training data sets [4], thereby exposing information that must be protected.

The issue of operational data validity must also be considered. In a military operation, the rate of

environmental change may be extremely high, meaning that data that was accurate hours or even minutes ago may already be outdated. If the AI system does not have reliable mechanisms for updating and verification, it may make a final decision based on an obsolete operational picture.

In this regard, data-related risks are not only technical. They can also directly affect the reliability of the command process and the integrity of the command chain. These risks require systematic measures for source verification, quality testing, anomaly detection, protection of sensitive and classified information, and limiting dependence on external or insufficiently transparent data streams.

C. Risks related to the algorithms and models

The models used in AI systems can be a source of significant vulnerabilities. One of the main problems is the transparency, especially the lack of it in complex models such as neural networks. The large algorithms and complex models are difficult to understand. They may provide an assessment or recommendation with high confidence, without it being clear which factors led to it. This makes it difficult to evaluate the reliability of the results and reduces operator trust. In the command structure, this is a serious limitation because the commander must not only receive a result but also have grounds to trust it or reject it. If the AI system cannot provide sufficiently clear logic behind its analysis, it risks becoming a “black box” that influences decisions without real possibilities for control [6], [8] and [10]. According to the U.S. Department of Defence, the lack of transparency in AI systems creates serious challenges for trust and control in command processes [8].

A serious threat is also posed by malicious model modifications, including model poisoning and backdoor attacks [3], [4]. In these scenarios, the model is compromised in such a way that under normal conditions, it functions as expected, but under certain input data or combinations of signals, it generates intentionally incorrect outputs. This is particularly dangerous because the compromise may remain hidden during standard testing and manifest itself at a critical moment.

D. Risks related to software and integration

AI solutions rarely exist as isolated modules. In practice, they belong to a broader software ecosystem that includes libraries, development frameworks, software dependencies, interfaces, databases, visualisation systems, and tools for communication with other platforms. It is precisely the complexity which increases the risk of vulnerabilities and compromise along the supply chain [3], [7]. If a software library contains a vulnerability, is maliciously modified, or becomes compromised during distribution, this may affect the final AI system as well. In environments where open-source tools are frequently used without sufficient verification, this risk is significant.

The integration of AI into C2 systems also represents a serious challenge. C2 systems are critical infrastructure for the armed forces, and the addition of AI components increases their complexity. Every new integration point (interface, API, data-exchange module, or external service) expands the attack surface. From here, an error or weakness

in a single component can lead to cascading failures across the entire C2 system.

The issue of compatibility and predictability must also be taken into account. Military systems are often built in different periods, by different manufacturers, and according to different standards. Adding AI functionalities to those environments may lead to unpredictable interactions, delays, data exchange errors, or disruption to existing control and protection mechanisms. Research by the NATO Cooperative Cyber Defence Centre of Excellence in the field of cybersecurity shows that AI components can become an independent vector for cyberattacks, especially when there is insufficient traceability of their origin and lifecycle [11]. In this sense, the security of AI cannot be separated from the security of the entire software architecture into which the AI is embedded.

E. Risks related to communication infrastructure

Communication infrastructure is also a critical element of command chains. Disruptions such as jamming, cyberattacks, and manipulation of the communication flow can lead to a distorted operational picture [5].

Many AI systems count on a continuous stream of input data, exchange between different levels of command, access to distributed databases, and synchronisation between multiple platforms and sensors, which makes them particularly vulnerable to such communication disturbances. There is also a risk of manipulation of the communication flow. If an adversary manages to inject false messages, alter information flow priorities, or introduce artificial noise into the communication link, this may affect both operators and AI systems. In the absence of adequate verification of the source and integrity of the data, this may lead to a distorted operational picture and to incorrect decision-making.

An additional problem is the dependence on external infrastructure - for example, cloud services, satellite channels, data centres, or inter-system connections controlled by third parties. In the military domain, such dependence may become a critical weakness if, during a crisis or conflict, access to these resources is restricted, compromised, or politically obstructed. Therefore, resilient communications are directly related to the reliability of AI.

F. Risks related to the human factor

Regardless of the degree of automation, the human factor remains a key element in command chains. The main risks include insufficient training, incorrect interpretation of results, and excessive trust in the systems.

The first issue concerns preparation and training. If operators and commanders do not sufficiently understand the logic, limitations, and conditions for using a given AI system, there is a risk of misinterpreting the results. They may accept a probabilistic assessment as a categorical fact, fail to recognise signs of anomalies, or use the system outside the scope for which it is intended.

An additional risk is excessive reliance on automated recommendations. The better an AI system performs in

routine or well-structured situations, the more likely operators are to begin over-trusting it. This phenomenon, known as *automation bias*, can weaken critical thinking and lead to decisions being made by mechanically following recommendations without sufficient contextual assessment and verification, which contradicts the principles of responsible AI use [8], [9], [10].

The opposite risk is distrust of the system, especially if it has low transparency or has produced inconsistent results in the past. In such a case, AI may be formally integrated into the command process, but in practice, it is not used effectively.

There is also an issue with the distribution of responsibility, especially when decisions are partially generated by AI. When AI participates in the decision-making process, it must be clear who bears responsibility for the final decision. This requires a clear definition of roles and responsibilities. If roles are not clearly distinguished, there is a risk of organisational gaps in which no one assumes full responsibility for the consequences. According to analyses by RAND Corporation, the balance between automation and human involvement is critical for the reliability of military decisions [9]. This requires the creation of integrated measures that cover all levels of the system.

G. Comparison with existing studies and implications

Existing studies on artificial intelligence in defence and cybersecurity primarily focus on specific dimensions of AI adoption, including trustworthy AI, ethical principles, adversarial machine learning, software vulnerabilities, and autonomous decision-making [3], [6], [8], [10], [11], [14]–[17]. These works provide valuable insights into individual categories of risks but often address them separately or within broader AI governance frameworks.

In contrast, the present study proposes an integrated perspective by analysing risks across interconnected components of military command chains, including data, algorithms and models, software integration, communication infrastructure, and the human factor. This system-oriented approach allows identification of how vulnerabilities propagate through different layers of the decision-making process rather than emerging as isolated technical issues.

The qualitative risk assessment presented in Table 2 additionally supports prioritisation of vulnerabilities according to their estimated probability and operational impact. This contributes to a more structured understanding of AI-related risks in military environments and may support future development of quantitative risk evaluation methods.

Therefore, the findings suggest that resilience in AI-enabled command chains depends not only on technological robustness but also on maintaining transparency, human oversight, and adaptability across the entire operational system.

IV. RISK MITIGATION APPROACHES

Effective and sufficient mitigation of the risks associated with integrating AI into command chains demands addressing vulnerabilities at both the system elements and across the decision-making cycle. The measures should cover all components and ensure technological resilience plus organisational reliability.

A. Data management and protection

Data quality is a fundamental requirement for the reliability of AI systems. It is necessary to establish strict data-management policies [3], [4], which include:

- verification of sources;
- validation of input data;
- detection of inconsistencies and anomalies;
- protection against manipulation (data poisoning).

Special attention should be paid to the processing of classified information. It is necessary to apply mechanisms for access control, cryptographic protection, and minimisation of exposed data.

B. Validation and transparency of models

AI models must undergo systematic validation, which includes:

- testing under different scenarios;
- checking resilience of the model against adversarial attacks;
- assessment of reliability and stability;
- traceability of the AI training process.

Regular testing and the use of explainable models increase trust and allow better control over decisions [6]. Where possible, methods for AI transparency (Explainable AI - XAI) should be used, as they allow better understanding of the logic behind the decisions being made. Even when complex models offer better performance, in situations involving critically important decisions, it is important for the commander to have at least some partially understandable logic explaining why a particular recommendation is given.

C. Software and integration security

The security of the software environment and the management of software risk require:

- control over the software dependencies, libraries, and external components used [7];
- regular vulnerability checks;
- the use of secure environments for development and deployment;
- clear separation between test and operational systems.

The integration of AI into existing military C2 systems must be gradual and carefully controlled, with minimisation of the attack surface. It is necessary to clearly

separate tests and operations, limit the permissions of AI modules to the minimum required, and to continuously monitor their behaviour after deployment.

D. Communication resilience

The communication infrastructure should be designed with a high degree of resilience [5], including:

- redundant channels and cryptographic protection;
- protection against jamming and cyberattacks;
- mechanisms for verifying the authenticity of messages;
- the ability to operate in a degraded communication environment.

AI systems must be able to function under partial data loss without generating misleading results. AI in command chains should be designed in such a way that it can operate under degraded communications and partial loss of connectivity, so that it does not become a source of uncertainty.

E. The human in the decision-making process

In accordance with the principles of NATO and the U.S. Department of Defence, the application of human-in-the-loop is a key requirement for critical decisions [5], [8], [10], [11], [12] and [13]. This principle is also important for ensuring the controllability of the system, and this includes:

- maintaining human control in critical decisions;
- training personnel to work with AI;
- development of critical thinking;
- clear definition of responsibilities.

AI should be viewed as a tool for support, not as a replacement for human final judgment. The human factor should not be seen as a weakness that must be "replaced" by automation, but as a key element that must be supported through training, clear definitions and procedures, and developed critical thinking, alongside proper positioning of AI as an assisting instrument.

V. CONCLUSIONS

The integration of AI into the command chains of the armed forces provides significant opportunities for increasing efficiency, accelerating analysis, and improving situational awareness. These advantages, however, are accompanied by complex risks that affect all components of the system.

The analysis shows that the most significant vulnerabilities are related to data quality, model trustworthiness, software security, communication resilience, and the role of the human factor. The interaction between these elements determines the overall resilience of the command chain.

Successful integration of AI requires a balanced approach that combines technological capabilities with clear mechanisms for control, transparency, and

responsibility. It is particularly important to preserve the leading role of the human [10] in the decision-making process, using AI capabilities for support rather than replacement.

The present study contributes by proposing a structured framework for analysing AI-related risks in military command chains. This framework may serve as a basis for developing standardised risk-assessment approaches and future quantitative evaluation methods for AI-enabled defence systems.

REFERENCES

- [1] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, 2021.
- [2] I. Goodfellow et al., *Deep Learning*, MIT Press, 2016.
- [3] Australian Cyber Security Centre, “Artificial Intelligence and Machine Learning Supply Chain Risks,” 2025. [Online]. Available: <https://www.cyber.gov.au/>
- [4] National Institute of Standards and Technology (NIST), “Adversarial Machine Learning: A Taxonomy and Terminology,” 2025. [Online]. Available: <https://www.nist.gov/>
- [5] NATO, “Summary of NATO's revised Artificial Intelligence (AI) strategy” 2024. [Online]. Available: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- [6] European Commission, “Ethics Guidelines for Trustworthy Artificial Intelligence,” 2019. [Online]. Available: <https://digital-strategy.ec.europa.eu/>
- [7] OWASP Foundation, “ML Security Top 10,” 2024. [Online]. Available: <https://owasp.org/www-project-machine-learning-security-top-10/>
- [8] U.S. Department of Defense, “Responsible Artificial Intelligence Strategy and Implementation Pathway,” 2022. [Online]. Available: <https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF>
- [9] RAND Corporation, “Artificial Intelligence and International Security,” 2020. [Online]. Available: <https://www.rand.org/>
- [10] U.S. Department of Defense, “DOD Adopts Ethical Principles for Artificial Intelligence” 2020. [Online]. Available: <https://www.war.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/>
- [11] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), “Artificial Intelligence, Cybersecurity and Warfare,” 2023. [Online]. Available: https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf
- [12] NATO, “Summary of the NATO Artificial Intelligence Strategy”, 2021, [Online]. Available: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy>
- [13] NATO Data and Artificial Intelligence Review Board (DARB), “Framework Documents,” 2023. [Online]. Available: https://cdn.asp.events/CLIENT_Defence_8EE24275_D70D_4386_936BB8991B847FF8/sites/Navv-Leaders-2022/media/libraries/cne24-presentations/Day-3-UDSA-1115-OPTION-1- PUBLIC_CNE_NATO_Data_and_AI_Policies.pdf
- [14] G. Falco et al., “Cybersecurity Risks in Artificial Intelligence Systems,” *Computer*, vol. 54, no. 6, pp. 84–88, 2021.
- [15] A. Taddeo and L. Floridi, “How Artificial Intelligence can be a Force for Good in Defence,” *Science and Engineering Ethics*, vol. 24, no. 6, pp. 1–15, 2020.
- [16] M. Brundage et al., “Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims,” *arXiv*, 2020.
- [17] M. Cummings, “Artificial Intelligence and the Future of Warfare,” Chatham House Research Paper, 2021.

Psychological Qualities of Strategic Leaders and Their Significance for Professional Selection in the National Security System

Valeri Ivanov

Institute of Defence "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
val.ivanov@abv.bg
ORCID: [0009-0004-8147-3762](https://orcid.org/0009-0004-8147-3762)

Kristiyan Petrov

Institute of Defence "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
kristiyanpetrov16@gmail.com
ORCID: [0009-0003-4198-750X](https://orcid.org/0009-0003-4198-750X)

Abstract—This report analyses the role of psychological qualities of strategic leaders as a critical determinant of the effectiveness, resilience, and legitimacy of the national security system. Security is approached not only as an institutional and normative framework but also as a function of the human factor, which plays a central role in strategic decision-making under conditions of uncertainty, risk, and crisis. Particular emphasis is placed on the need to integrate scientifically grounded psychological criteria into the professional selection of leadership personnel, including emotional and moral resilience, cognitive flexibility, self-regulation, and reflexivity. The analysis is grounded in contemporary theoretical perspectives on strategic leadership and management psychology and highlights the importance of a systematic psychological selection framework for the sustainable functioning of security institutions.

Keywords—strategic leadership, cognitive flexibility, moral resilience, psychological resilience

I. INTRODUCTION

In the contemporary security environment, strategic leadership has established itself as a key factor for the sustainable functioning of state institutions. The processes of globalization, increasing geopolitical instability, hybrid threats, information and cyber operations, as well as heightened public tension pose new and increasingly complex challenges to the national security system. In this environment, security management requires not only effective institutional mechanisms but also strategic leadership capable of operating under conditions of risk, uncertainty, and crisis.

Strategic leaders within the national security system are required not only to possess a high level of professional and expert training but also to demonstrate clearly defined psychological fitness. Managerial decisions in this field are associated with a high degree of responsibility, have long-

term consequences, and exert a direct impact on public trust and the legitimacy of institutions. As Slatinski [4], [5], [6] notes, security cannot be viewed solely as a technical or normative problem, but rather as a complex social process in which the human factor plays a decisive role.

The analysis of practices for the selection and development of managerial personnel in the national security system reveals the presence of significant deficits related to the absence of a unified, scientifically grounded framework for assessing the psychological qualities of strategic leaders. In a number of cases, personnel decisions are based on formal criteria, administrative continuity, or political expediency, without taking into account psychological suitability for holding strategic managerial positions [1], [2].

Such an approach creates prerequisites for managerial instability, reduced effectiveness of institutional decisions, and erosion of public trust in security structures. This necessitates an in-depth theoretical analysis of the psychological qualities of strategic leaders and their consideration as an essential element of professional selection.

The purpose of the present report is to analyse the significance of the key psychological qualities of strategic leaders and to substantiate the necessity of their institutionalization as a central element in the process of professional selection within the national security system.

II. MATERIALS AND METHODS

The study is based on a qualitative theoretical analysis of established concepts in leadership theory and management psychology. A comparative approach is applied to examine different models of leadership effectiveness and their relevance to the national security context.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.26>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

The research relies on a review of key academic sources related to emotional intelligence, strategic leadership, and organizational behaviour. The analysis focuses on identifying recurring psychological constructs and evaluating their applicability to high-risk decision-making environments.

Additionally, a contextual approach is used to adapt these theoretical frameworks to the specific conditions of the national security system, taking into account institutional dynamics, uncertainty, and crisis management requirements.

III. RESULTS AND DISCUSSION

The analysis of the scientific literature and theoretical models indicates that the effectiveness of strategic leadership in the national security system is strongly dependent on a specific set of psychological qualities. These qualities form an integrated psychological profile that determines the leader's ability to act under conditions of uncertainty and institutional pressure.

The key psychological qualities identified in this study are emotional resilience, cognitive flexibility and strategic thinking, moral resilience and ethical orientation, and self-awareness and reflexivity. These characteristics are interdependent and collectively contribute to sustainable and effective leadership behaviour.

A. Key Psychological Qualities of Strategic Leaders

In the scientific literature, there are various approaches to defining the psychological qualities of effective leaders within security systems [4], [8], [10]. However, there is a lack of a unified and systematized model that can be directly applied to the conditions of national security in the Bulgarian context.

Based on an analysis of established theoretical concepts and taking into account the specifics of strategic management within the national security system, the present report assumes that the key psychological qualities of strategic leaders are: emotional resilience, cognitive flexibility and strategic thinking, moral resilience and ethical orientation, and self-awareness and reflexivity.

These qualities are not viewed in isolation, but as an interrelated psychological profile that determines an individual's suitability for occupying a strategic leadership position.

B. Emotional Resilience

In classical leadership studies, emotional resilience is viewed as an individual's ability to maintain psychological stability, self-control, and consistency of behaviour under conditions of tension, stress, and conflict situations [8]. In this context, resilience is associated with the predictability of managerial responses and with the leader's capacity to make rational decisions even under strong external and internal pressure.

Goleman [9] expands this understanding by considering emotional resilience as a key component of emotional

intelligence. According to him, the ability for self-regulation, control over impulsive reactions, and awareness of one's own emotional states is an essential prerequisite for effective leadership behaviour. In this sense, emotional resilience is not limited solely to "stress tolerance," but includes the active management of emotions in the interest of managerial objectives.

The present analysis adopts these theoretical propositions but emphasizes that, under conditions of national security, emotional resilience has a deeper and more structural significance. Here, it should not be viewed solely as an individual personality trait, but as a factor that directly influences the sustainability of institutional decisions and trust in strategic management. As Slatinski [4] notes, the human factor is a key element of security, and unstable leadership behaviour can become a source of systemic risk.

Within the national security system, managerial decisions are often made under conditions of high uncertainty, limited information, and significant public and political pressure. In such an environment, the emotional instability of a strategic leader may lead to impulsive reactions, inconsistency in managerial actions, and impaired institutional coordination. This, in turn, compromises not only the specific decision but also the legitimacy of governance as a whole.

In the Bulgarian context, the importance of emotional resilience is even more pronounced. Strategic leaders operate in an environment characterized by a high degree of politicization, public distrust in institutions, and limited resource capacities. In such a setting, the lack of emotional resilience increases the risk of reactive rather than strategic management, in which decisions are made under the influence of momentary emotional states or external pressure.

For all these reasons, it can be confidently stated that emotional resilience should be regarded as a fundamental and mandatory psychological quality in the selection of strategic leaders within the national security system. It cannot be compensated for through professional experience or formal expertise, as it represents a deeply rooted personality characteristic that determines how a leader functions in critical situations.

C. Cognitive Flexibility and Strategic Thinking

In leadership theories, cognitive flexibility is viewed as an individual's ability to adapt their thinking strategies depending on changing conditions and to integrate different, often contradictory perspectives when analysing complex situations. Sternberg [11] defines this quality as a key component of effective thinking, which enables the overcoming of rigid cognitive schemes and creates conditions for a creative and analytical approach to problem solving.

Yukl [10] directly links cognitive flexibility to leaders' ability to make decisions under conditions of uncertainty, incomplete or contradictory information, and a dynamic environment. According to him, strategic leaders rarely have a complete picture of the situation, which necessitates continuous reconsideration of initial assessments and adaptation of managerial decisions during their implementation.

The author's position in the present report is that, for strategic leaders in the national security system, cognitive flexibility has primarily a functional, rather than merely an intellectual, significance. It is not limited to a high level of intellectual abilities or analytical skills, but represents a practical capacity for timely adaptation of strategies and managerial approaches in response to the changing security environment. As Tarkanalanov [7] emphasizes, effective strategic analysis in the security system requires not only expert knowledge, but also readiness to revise already adopted assessments and scenarios.

Under conditions of national security, cognitive flexibility enables the strategic leader to avoid strategic rigidity and dogmatism, which often manifest as adherence to established patterns of thinking even when the objective environment renders them ineffective. The lack of cognitive adaptability increases the risk of delayed or inadequate managerial responses, especially in crisis situations where decision-making time is limited and the consequences of errors are significant.

In the Bulgarian context, the importance of cognitive flexibility is further amplified by the specifics of the institutional environment. Frequent structural changes, a dynamic regulatory framework, and limited predictability of the security environment require strategic leaders to possess the ability for rapid orientation and adaptation. Under such conditions, strategic thinking cannot be static or pre-fixed, but should be based on a continuous process of analysis, evaluation, and adjustment.

All of the above allows for the advancement of the thesis that cognitive flexibility and strategic thinking should be regarded as interrelated and mandatory components of the psychological profile of the strategic leader. They represent a key criterion in professional selection, as it is precisely through them that the capacity for sustainable and adequate governance is ensured in the conditions of a complex and dynamic national security environment.

D. Moral Resilience and Ethical Orientation

Today, moral resilience is viewed as a key component of the legitimate exercise of power. Ciulla [12] places ethical orientation at the center of leadership, emphasizing that managerial effectiveness cannot be separated from its moral justification. According to this approach, leadership is not limited to achieving results, but includes responsibility toward institutions, society, and the value framework within which managerial decisions are made.

Bass [8] considers moral resilience as a foundation for building trust and organizational stability. In this context, the leader's ethical consistency creates predictability in managerial behaviour and contributes to the sustainability of organizational culture. The absence of clearly defined moral guidelines leads to the substitution of professional criteria with personal or situational considerations, which undermines trust in leadership.

The present report adopts these theoretical propositions, but argues that they should be examined through the prism of national security, where moral resilience acquires additional, systemic significance. In this field, managerial decisions do not affect solely organizational effectiveness, but have a direct impact on the rule of law, public trust, and the legitimacy of state institutions. As Ivanov [1] notes, security is inconceivable without institutional legitimacy, which in turn is directly linked to the moral consistency of strategic leadership.

Under conditions of political and institutional pressure, moral resilience manifests as the strategic leader's ability to preserve value-based autonomy and to make decisions in accordance with legal and ethical norms, even when this contradicts short-term interests or external expectations. The lack of a clearly articulated ethical orientation in such an environment creates prerequisites for personnel distortions, informal dependencies, and erosion of public trust in security structures.

In our conditions, the importance of moral resilience is particularly pronounced due to historically accumulated problems with institutional trust and the high sensitivity of society to the actions of security structures. In this sense, moral resilience cannot be viewed as an abstract value or as a secondary quality, but as a practical condition for the legitimate functioning of the national security system.

All of this leads to the conclusion that moral resilience and a clearly expressed ethical orientation should be regarded as a mandatory and leading criterion in the selection of strategic leaders. They can also hardly be compensated for through professional expertise or managerial experience, as they represent the value foundation upon which sustainable and legitimate leadership is built.

E. Self-Awareness and Reflexivity

In contemporary theories of leadership and social governance, self-awareness is regarded as a fundamental psychological quality that enables the leader to recognize their own emotional states, cognitive limitations, and established behavioral patterns. Goleman [9] defines self-awareness as the foundation of effective self-regulation and as a key element of personal maturity, without which managerial behavior can hardly be sustainable and predictable.

Reflexivity, in turn, is expressed in the leader's ability to critically reflect on their own actions, decisions, and mistakes made, as well as to draw lessons from managerial experience. Milushev [3] emphasizes the importance of this quality for crisis management, noting that the lack of

reflexivity increases the likelihood of repeating strategic errors and deepening crisis processes.

It is considered that self-awareness and reflexivity should be viewed as a mechanism of self-correction of strategic leadership. They provide an opportunity to adapt managerial behaviour not through external coercion or formal control, but through internal awareness and a critical attitude toward one's own decisions. In this sense, these qualities play a key role in the long-term sustainability of leadership.

Under conditions of national security, the significance of self-awareness and reflexivity is particularly pronounced. Strategic leaders operate in an environment characterized by high responsibility, limited transparency, and significant institutional pressure. In such an environment, a leader who does not recognize their own limitations and is not capable of self-critical assessment is more prone to strategic errors, authoritarian managerial practices, and gradual institutional isolation.

The lack of self-awareness and reflexivity often manifests through rejection of feedback, ignoring alternative viewpoints, and a tendency toward self-confirming thinking. This behaviour limits the possibilities for correcting managerial decisions and increases the risk of accumulating systemic errors with long-term consequences for the functioning of security institutions.

For these reasons, for the purposes of the present report it can be assumed that self-awareness and reflexivity should be regarded as essential and mandatory elements of the psychological profile of the strategic leader. They not only complement the other psychological qualities, but also provide the internal mechanism through which the leader maintains adaptability, consistency, and sustainability of managerial behaviour in the conditions of a dynamic and risk-prone national security environment.

IV. CONCLUSION

The present report examines the psychological qualities of strategic leaders not as an abstract set of personality characteristics, but as a systemic resource for the sustainable functioning of the national security system. The conducted theoretical analysis demonstrates that the effectiveness and legitimacy of strategic governance depend to a decisive extent on the psychological profile of the leaders who make decisions under conditions of risk, uncertainty, and high public responsibility.

On the basis of established theoretical approaches and taking into account the specifics of national security, the report substantiates an authorial position according to which the key psychological qualities of strategic leaders are emotional resilience, cognitive flexibility and strategic thinking, moral resilience and ethical orientation, as well as self-awareness and reflexivity. These qualities are not viewed in isolation, but as an interrelated system that determines the leader's ability to maintain consistent, adaptive, and legitimate managerial behaviour.

The author's thesis in the present report is that the systematic integration of these psychological qualities into the process of professional selection of strategic leaders constitutes an essential condition for enhancing the effectiveness and sustainability of the national security system. Selection based solely on formal criteria and professional experience is not sufficient if it does not take into account the psychological suitability of the individual for functioning under conditions of strategic governance.

V. ACKNOWLEDGMENTS

The present report was implemented with the support of the Ministry of Education and Science within the framework of the National Scientific Program "Security and Defence," adopted by Council of Ministers Decision No. 731 of 21.10.2021, and in accordance with Agreement No. D01-74/19.05.2022.

REFERENCES

- [1] V. Ivanov, Protection of the State Border and the New World Order. Sofia: Military Publishing House, 2005.
- [2] V. Ivanov, Intelligent National Security System. Capabilities, Approaches, Solutions. Sofia: "Boryana Group", 2014.
- [3] L. Milushev, The Crisis – Managerial Aspects and Opportunities. Plovdiv: Europres, 2008.
- [4] N. Slatinski, Dimensions of Security. Sofia, 2000.
- [5] N. Slatinski, Aspects, Analyses, Alternatives. Sofia, 2004.
- [6] N. Slatinski, The Five Levels of Security. Sofia: Military Publishing House, 2010.
- [7] Y. Tarkanalanov, Intelligence Analysis. Sofia: "Albatros", 2005.
- [8] B. M. Bass, Handbook of Leadership: Theory, Research, and Managerial Applications. New York: Free Press, 1990.
- [9] D. Goleman, Emotional Intelligence: Why It Can Matter More Than IQ. New York: Bantam Books, 1995.
- [10] G. Yukl, Leadership in Organizations. Boston: Pearson Education, 2013.
- [11] R. J. Sternberg, Thinking Styles. Cambridge: Cambridge University Press, 1997.
- [12] J. B. Ciulla, Ethics, the Heart of Leadership. Westport, CT: Praeger, 2004.

Electromagnetic Protection Using Software-Defined Radio

Ivan Ivanov

C4I Systems Development Directorate
Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
i.p.ivanov@di.mod.bg

Sevdalin Spasov

C4I Systems Development Directorate
Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
s.spasov@di.mod.bg

Abstract: The main elements of electromagnetic protection (EP) such as ensuring electromagnetic compatibility measures, communication equipment protection measures, electromagnetic radiation management, preventive countermeasures against enemy radio intelligence have been examined. A definition, basic terms and the architecture of software-defined radio (SDR) have been given. SDR implementation possibilities at electromagnetic protection of military communication systems have been considered. The paper also includes a GNU Radio proof-of-concept simulation of SDR-based spatial signal analysis and discusses practical coherence challenges when moving from simulation to a multi-device SDR implementation.

Keywords: Electromagnetic warfare (EW), electromagnetic protection (EP), Software-defined radio (SDR).

• INTRODUCTION

During the last three decades, the most powerful armies have continued to dominate the electromagnetic spectrum over the enemies and adversaries who lack the ability to challenge their technological superiority. However, in recent years, regional peers have demonstrated formidable capabilities in hybrid operational environments, including electromagnetic spectrum. These capabilities have been also demonstrated in the ongoing conflict in Ukraine mainly in the form of jamming of communications, global navigation satellite system (GNSS) and control systems of military drones.

Combat platforms are built with a wide application of electronic devices and systems. A large part of these systems receives and transmit both data and control signals. These data and signals are transmitted and received using electromagnetic waves. The use of the electromagnetic spectrum makes them vulnerable to interference by the enemy [6]. All this assumes the growing importance of electromagnetic warfare (EW) in recent military conflicts.

• ESSENCE OF ELECTROMAGNETIC PROTECTION (EP) AND ITS PLACE IN ELECTROMAGNETIC WARFARE

○ Electromagnetic Warfare and its components

The Electromagnetic Warfare (EW) is adopted as a main term in this paper and it is used in the entire text. Electromagnetic Warfare is one of the main warfare domains.

Electromagnetic warfare [1, 2] is the use of electromagnetic energy to provide situational awareness and achieve offensive and defensive results, and to ensure superiority in the electromagnetic spectrum. EW (Fig. 1) consists [1, 2, 3, 4] of three main elements.

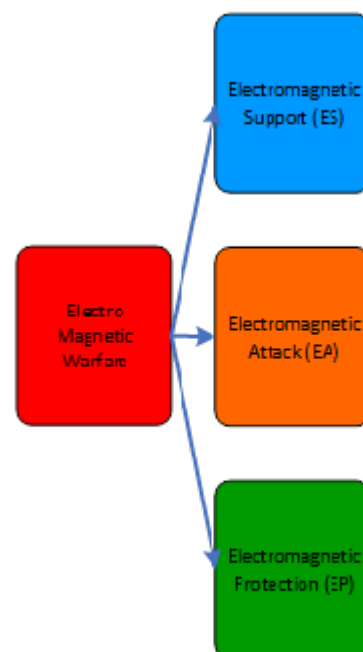


Fig.1 Electromagnetic Warfare's components

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.156>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

○ *The essence, and main elements of the Electromagnetic Protection (EP)*

Electromagnetic Protection is a complex of technical and organizational measures using electromagnetic energy to provide protection and effective use of the electromagnetic spectrum by allied forces, carried out in order to ensure the stable operation of their own systems and means of controlling troops and weapons, in conditions of electronic effects from the enemy.

From an engineering point of view, EP can be understood as a set of measures that reduce the effect of intentional and unintentional electromagnetic interference. These measures include protection against jamming, protection against deception and signal spoofing, reduction of the probability that friendly emissions will be intercepted or detected, electromagnetic compatibility, emission control, spectrum management, and adaptation of systems to new threats.

For the purpose of this analysis, EP is treated as a functional engineering taxonomy rather than as a strict doctrinal hierarchy. From this point of view the EP consists of six main components:

- Anti-jam protection
- Anti-deception / anti-spoofing
- Low probability techniques
- EMI / EMC protection
- Emission control and spectrum management
- Adaptive protection

Each EP component has subcomponents. The deeper EP structure will be considered further in order to organize the protective functions that are relevant to SDR-based implementation.

- CHALLENGES IN ELECTROMAGNETIC PROTECTION OF MILITARY COMMUNICATION SYSTEMS. GENERAL INFORMATION ABOUT SOFTWARE-DEFINED RADIO (SDR)

○ *Challenges in electromagnetic protection of military communication systems*

Electromagnetic protection (EP) is conducted by electromagnetic warfare units in modern armies. EP has the character of a systematic activity, because it encompasses constructive, technical and organizational measures for protection. Therefore, electromagnetic protection can achieve its maximum effectiveness in EW formations.

On the other hand, electromagnetic protection (EP) in the communication formations of modern armies is not organized on the systematic basis. For example, only a part of the electromagnetic protection functions are built into the communication equipment in terms of circuitry. They include both measures for reducing the output power and readjusting the operating frequency of the transmitters, as well as various schemes for automatically adjusting the gain in their receivers. In this state of arts, the communication equipment does not have a built-in

function for detecting interference. Thus, their receivers cannot automatically determine the fact of the presence of interference in order to take the appropriate protection measures. In order to detect the presence of interference and take protection measures, the presence of an operator is necessary.

The combat operations and the radio-electronic environment changes very quickly at the tactical level of the armed forces. Therefore, rapid and adequate technical and organizational actions are required to protect communication means. The detection and analysis of natural and artificial interference in the troops is within the competence of electronic intelligence units. These units are at operational or strategic level, since the results of the analysis of intercepted enemy emissions are used by commanders at these levels. Therefore, communication units at the tactical level do not have an automatic system for detecting, analyzing and responding to intentional interference (jamming). In order to take protective measures, the intervention of an operator is necessary. However, this measure necessarily requires the presence of an operator and his constant monitoring of the radio-electronic environment. This cannot always be done with the necessary speed and reliability. From all that has been said so far, the conclusion is that communication units at the tactical level must have an automatic or automated system for detecting, analyzing, and responding to intentional interference (jamming).

One possible technical solution to this problem could be the use of software-defined radio (SDR).

○ *General information about software-defined radio (SDR)*

Software Defined Radio is a suitable technological platform for implementing a significant part of EP functionality because it enables programmable and reconfigurable signal processing. This is due to its structure and properties.

Software-defined radio is a modern paradigm for the practical implementation of radio communication systems. The foundations of the “software-defined radio” (software-defined radio - SDR) paradigm are associated with the research of DARPA and the US Air Force under the SpeakEasy project in the early 1980s on the creation of a prototype radio station [7] covering the range from 2 MHz to 2 GHz and implementing about 10 communication standards [8]. Part of the results obtained in the field of system architecture were published by Mitola in the early 1990s, where the author [9] introduced the concepts [10] “software radio” and “software-defined radio” [11]. Each professional organization attempts to define a common framework of terms and definitions to allow for easy communication among professionals working in a common field. In the field of software-defined radio communications, the Institute of Electrical and Electronics Engineers (IEEE), through its working group P1900.1, has created definitions (Table I) to ensure that everyone in the field has a common terminology. A key definition in this brief ontic is that of “software-defined radio”: a radio in which some or all of the physical layer functions are software-defined.

The definitions introduced allow not only to standardize the concept of SDR, but also to create a context in which this concept “lives”. This allows the formation of other contexts in which SDR can be attributed to different entities.

A structural-functional block diagram of such a radio is shown in Fig. 2.

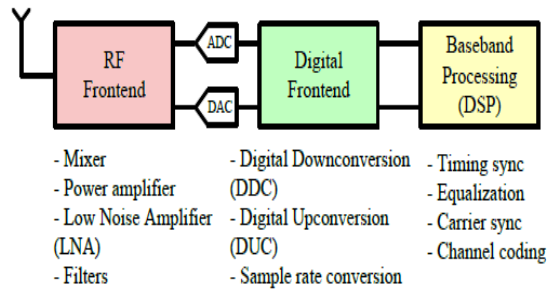


Fig.2 Structural-functional block diagram of SDR

One of the main differences between the architecture of a software-defined radio and an ideal one is the presence/need of a radio frequency front-end operating in the analogue space and implementing such functions as mixing, low-noise amplification, analogue filtering, etc. Another architectural feature of modern SDRs is the implementation of digital processing by two digital blocks – a digital front-end and a baseband digital signal processing block. The first block performs all conversions from transmitted signal to baseband (and vice versa) and those related to the clock frequency (frequency compression, expansion, etc.). The second block performs all conversions to baseband and is typically implemented by a general-purpose computer or a single-board microcomputer.

The analogue RF front-end, ADC, DAC and digital front-end are combined into a common building block – RF digital front-end in current products on the market that allow prototyping in the field of SDR. This leads to the generalized, mass, modern SDR architecture shown in Fig. 3.

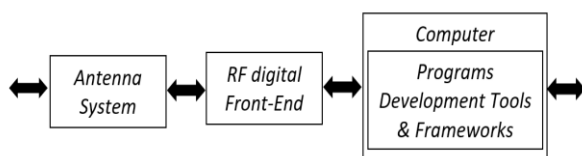


Fig.3 Generalized mass architecture of SDR

The SDR technology is supported by numerous software packages for computer modelling and simulation. The most famous of them are: Matlab, GNU Radio, LabVIEW, etc. The advantage of using such packages is the rapid transition from a computer module to a practical implementation

• SDR IMPLEMENTATION POSSIBILITIES IN ELECTROMAGNETIC PROTECTION OF MILITARY COMMUNICATION SYSTEMS

○ SDR as a platform for EP

SDR is a suitable technological platform for implementing a significant part of EP functionality because it enables programmable and reconfigurable signal processing. Through SDR, it is possible to implement adaptive waveforms, frequency agility, spread spectrum techniques, digital filtering, spectrum sensing, interference detection, modulation and coding adaptation, and algorithms for identifying spoofing or deception attempts.

The deeper EP structure below is a practical way to organize the protective functions that are relevant to SDR-based implementation. The Table 1 demonstrates the role of SDR in the individual elements of EP.

THE ROLE OF SDR IN THE INDIVIDUAL ELEMENTS OF EP

1. ANTI-JAM PROTECTION

EP element	Short explanation	How SDR helps
Anti-jam protection	Protection against intentional jamming in order to preserve communication, navigation, or reception of the useful signal.	SDR enables frequency agility, adaptive parameter changes, interference detection, and switching to a more robust operating mode.
Frequency hopping	Fast or pseudorandom change of the operating frequency to make jamming and interception more difficult.	SDR can change the carrier frequency programmatically according to a predefined or adaptive hopping sequence.
Spread spectrum	Spreading the signal over a wider bandwidth to improve robustness and reduce spectral power density.	SDR can generate and receive DSSS, FHSS, chirp spread spectrum, and other spread spectrum waveforms.
Adaptive filtering	Suppression of narrowband, wideband, or impulsive interference by means of digital filters.	SDR can implement notch filters, adaptive FIR/IIR filters, spectral excision, and interference cancellation.
Beamforming null steering	Steering receiver sensitivity toward the useful signal and placing spatial nulls toward interference sources.	With a multichannel phase-coherent SDR, digital beamforming, direction-of-arrival estimation, and spatial jammer suppression can be implemented.
Coding, interleaving, redundancy	Increasing robustness against errors, burst interference, and partial signal loss.	SDR allows software-defined changes of FEC schemes, code rate, interleaving depth,

<i>EP element</i>	<i>Short explanation</i>	<i>How SDR helps</i>	<i>EP element</i>	<i>Short explanation</i>	<i>How SDR helps</i>
		repetitions, and fallback modes.		adversary receiver.	ES signals with low spectral power density.
2. ANTI-DECEPTION / ANTI-SPOOFING					
<i>EP element</i>	<i>Short explanation</i>	<i>How SDR helps</i>	LPD - Low Probability of Detection	Reducing the probability that the emission itself will be detected.	SDR enables control of power, duration, frequency, bandwidth, and the temporal pattern of the emission.
Anti-deception / anti-spoofing	Protection against false, misleading, or manipulated signals.	SDR enables analysis of time, frequency, phase, power, and correlation consistency, as well as anomaly detection in the received signal.	LPJ - Low Probability of Jam	Making effective jamming of the signal more difficult.	SDR enables adaptive change of waveform, frequency, coding, data rate, and operating mode.
Signal authentication	Verification that a signal or message originates from a legitimate source.	SDR can carry and process authenticated waveforms, but reliable authentication also requires cryptographic architecture and key management.	Emission shaping	Shaping the spectral, temporal, or spatial profile of the emission.	SDR can control spectral masks, envelope shaping, pulse shaping, duty cycle, and other parameters of the transmitted signal.
4. EMI / EMC PROTECTION					
<i>EP element</i>	<i>Short explanation</i>	<i>How SDR helps</i>	EMI / EMC protection	Protection from unintentional electromagnetic interference and ensuring compatibility between friendly systems.	SDR helps through spectrum monitoring, interference detection, adaptive filtering, and selection of a cleaner channel, but hardware EMC protection remains a separate requirement.
Consistency checks	Checks between expected and measured signal parameters.	SDR can compare Doppler, phase, time of arrival, power, correlation peaks, and other features to detect inconsistencies.	Filtering	Limiting or suppressing unwanted frequency components.	SDR implements digital filtering, but it often needs to be complemented by hardware RF filters before the ADC.
Multi-sensor validation	Confirmation of information through comparison with independent sensors or channels.	SDR can provide radio-channel measurements that are compared with GNSS, inertial navigation, other frequencies, or external sensors.	Shielding	Shielding sensitive electronic blocks from external electromagnetic effects.	SDR does not replace shielding, but it can support diagnostics by measuring residual interference and spectral contamination.
False-target rejection	Rejection of false targets or misleading responses, especially in radar and navigation systems.	SDR enables analysis of waveform parameters, delays, Doppler, correlation structure, and mismatch between expected and received signals.	Grounding	Proper grounding to reduce noise, parasitic currents, and interference.	SDR does not implement grounding, but it can be used to measure and evaluate the influence of noise and parasitic interference on the received signal.
3. LOW PROBABILITY TECHNIQUES					
<i>EP element</i>	<i>Short explanation</i>	<i>How SDR helps</i>	Frequency coordination	Coordination of used frequencies to avoid mutual interference.	SDR can monitor spectrum occupancy and support the selection of suitable operating frequencies.
Low probability techniques	Techniques that reduce the probability that a signal will be intercepted, detected, or successfully jammed.	SDR enables programmable control of waveform, power, bandwidth, time profile, and emission mode.			
LPI - Low Probability of Intercept	Reducing the probability that the signal will be intercepted by an	SDR can generate noise-like, wideband, short-duration, or frequency-mobile			

5. EMISSION CONTROL AND SPECTRUM MANAGEMENT

<i>EP element</i>	<i>Short explanation</i>	<i>How SDR helps</i>	<i>Short explanation</i>	<i>How SDR helps</i>
Emission control and spectrum management	Management of friendly emissions and the used frequency resources.	SDR enables software control of frequency, power, mode, bandwidth, time windows, and emission profile.		modulation, and coding.
EMCON	Control of when, for how long, and under what conditions the system emits.	SDR can switch between active, restricted, burst, passive, or listen-only modes.		
Restricted frequency lists	Lists of frequencies that must be avoided or protected.	SDR can apply programmed restrictions on allowed frequencies and automatically exclude prohibited or vulnerable channels.		
Power control	Control of transmitted power according to the mission and electromagnetic environment.	SDR can dynamically control transmit power through digital and RF control loops, within the limits of the hardware.		
Time/frequency planning	Planning when and on which frequencies the system should transmit or receive.	SDR can execute predefined or adaptive time-frequency plans.		

6. ADAPTIVE PROTECTION

<i>EP element</i>	<i>Short explanation</i>	<i>How SDR helps</i>
Adaptive protection	Adaptation of protective modes according to the electromagnetic environment and the type of threat.	SDR is especially suitable because it allows rapid changes of algorithms, waveforms, filters, frequencies, coding, and modes.
EW reprogramming	Updating parameters, modes, and algorithms in response to new threats.	SDR allows updates of waveforms, filters, classifiers, frequency plans, and protocols through software or FPGA reconfiguration.
Threat library updates	Updating databases of signatures, parameters, and models of threats.	SDR can collect IQ data and spectral features that support the update of classifiers and threat libraries.
Mode switching	Switching between different operating modes according to conditions.	SDR can switch between normal, anti-jam, LPI/LPD, emergency, low-rate, or passive modes.
Cognitive/adaptive radio techniques	Use of sensing, assessment, and automatic parameter selection according to the environment.	SDR provides the basis for spectrum sensing, decision logic, and adaptive selection of frequency, waveform,

In summary, SDR is most applicable to those parts of EP that depend on digital signal processing, adaptability, and reconfigurability [5]. It is particularly effective for anti-jam protection, spread spectrum, frequency hopping, adaptive filtering, low probability techniques, and adaptive protection. Its limitations are most significant in the purely hardware-related aspects of EP, such as shielding, grounding, RF preselection, hardware EMC protection, and physical robustness of the receiver front-end.

○ *Why SDR cannot implement the entire EP domain by itself*

SDR should not be treated as the complete EP system by itself. It is better understood as the core of an adaptive EP architecture. It provides flexibility, reconfigurability, and intelligent signal processing, but it must be complemented by appropriate RF hardware, antennas, EMC/EMI measures, cryptographic protection, and organizational control of electromagnetic emissions.

Several EP functions are primarily hardware-dependent or system-level in nature. For example, if a powerful jammer saturates the RF front-end before the analog-to-digital converter, the digital processing inside the SDR may no longer be able to recover the useful signal. In such cases, protection depends on RF preselectors, limiters, filters, high-dynamic-range receivers, automatic gain control, and careful front-end design.

Similarly, beamforming and null steering require more than software. They require a multichannel, phase-coherent SDR architecture, a suitable antenna array, common timing and frequency references, and calibration of the RF channels. EMI/EMC protection also requires shielding, grounding, cabling discipline, hardware filtering, and good RF and PCB design. Authentication and secure communication may use SDR waveforms, but reliable protection also requires cryptographic architecture, key management, trusted firmware, and platform security.

• SIMULATION AND IMPLEMENTATION ISSUES OF SDR-BASED SPATIAL SIGNAL ANALYSIS

This section complements the functional mapping of SDR capabilities by considering one selected capability in more detail: spatial signal analysis based on angle-of-arrival (AoA), also commonly referred to as direction-of-arrival (DOA), estimation. The section combines a GNU Radio proof-of-concept simulation with implementation-related issues that appear when the same processing chain is moved toward a physical multichannel SDR realization. The simulation is therefore used not as a complete electromagnetic protection (EP) demonstration, but as a controlled example of how SDR can support source localization, spatial consistency checking, beamforming/null-steering preparation, and anti-deception/anti-spoofing indication.

○ AoA model and practical MUSIC algorithm

In a multichannel receiver, AoA estimation exploits the phase differences observed at spatially separated antenna elements. For a narrowband far-field emitter, the received signal vector at a uniform linear array (ULA) can be represented by a steering vector whose phase progression depends on the inter-element spacing and the arrival angle. This is the basic physical mechanism used by practical algorithms such as MUSIC [12].

$$\mathbf{x}[n] = \mathbf{A}\mathbf{s}[n] + \mathbf{w}[n] \quad (1)$$

In (1), the vector $\mathbf{s}[n]$ contains the source signals, $\mathbf{A}$ is the array steering matrix, $\mathbf{x}[n]$ contains the samples observed at the antenna elements, and $\mathbf{w}[n]$ represents noise and disturbances. For an M -element ULA with normalized inter-element spacing d , the m -th component of the steering vector for an emitter arriving from angle θ can be written as:

$$a_m(\theta) = e^{-j2\pi m d \sin \theta} \quad (2)$$

where $m = 0, \dots, M - 1$. For several emitters, the steering matrix is formed by collecting the steering vectors corresponding to the individual source directions:

$$\mathbf{A} = [\mathbf{a}(\theta_1) \ \mathbf{a}(\theta_2) \ \dots \ \mathbf{a}(\theta_D)] \quad (3)$$

where D is the assumed number of spatially separable sources. The practical MUSIC procedure starts from the estimation of the spatial covariance matrix using N samples collected from the antenna channels:

$$\mathbf{R}_x = \frac{1}{N} \mathbf{X} \mathbf{X}^H \quad (4)$$

The covariance matrix is decomposed into signal and noise subspaces by eigenvalue decomposition. The eigenvectors associated with the largest eigenvalues span the signal subspace, while the remaining eigenvectors form the noise subspace:

$$\mathbf{R}_x = \mathbf{E}_s \mathbf{\Lambda}_s \mathbf{E}_s^H + \mathbf{E}_n \mathbf{\Lambda}_n \mathbf{E}_n^H \quad (5)$$

The MUSIC pseudo-spectrum is then evaluated by testing candidate steering vectors against the noise subspace. Peaks of the pseudo-spectrum indicate directions whose steering vectors are nearly orthogonal to the estimated noise subspace:

$$P_{\text{MUSIC}}(\theta) = \frac{1}{\|\mathbf{E}_n^H \mathbf{a}(\theta)\|^2} \quad (6)$$

In practical implementations, the number of assumed sources D must be configured or estimated. In the GNU Radio implementation used in this work, the source dimension is a configuration parameter of the DOA MUSIC block. This parameter determines the dimension of the signal subspace and, consequently, the dimension of the noise subspace used in (6).

○ GNU Radio simulation setup and preliminary DOA estimation results

The GNU Radio flowgraph models a four-element ULA. The Signal Source blocks represent independent simulated emitters, while the Multiply by Matrix block applies the steering matrix and generates the four antenna-channel signals. Therefore, the inputs of the matrix block

correspond to signal sources, whereas its outputs correspond to the antenna elements. The resulting antenna-channel streams are converted into vectors and processed by the DOA MUSIC block.

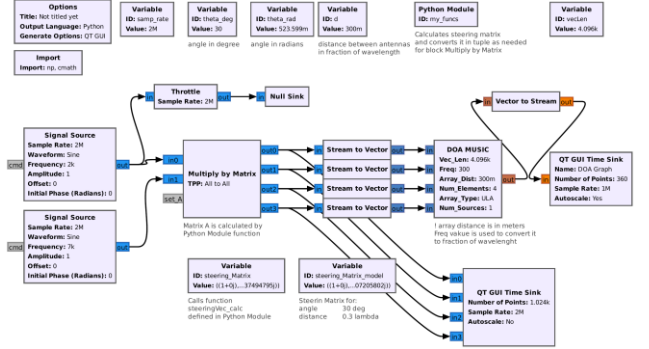


Fig. 4. GNU Radio flowgraph for simulated multichannel SDR-based spatial signal analysis.

For the simulation, the array type is ULA, the number of antenna elements is four, and the inter-element spacing is 0.3λ . The vector length used by the MUSIC processing block is 4096 samples, and the sample rate of the GNU Radio flow graph is 2 MS/s. In the reference scenario, a single source is placed at 30° . In the two-source scenario, a second source is introduced at 80° , while the reference source remains at 30° .

In the single-source case, the steering matrix contains one active steering vector and the MUSIC block is configured for one source. Within an unambiguous observation sector, the expected result is one dominant pseudo-spectrum peak near 30° . However, because the simulated array is a ULA and the displayed scan covers the full 0° – 359° angular interval, a mirror peak may also appear. This effect is a geometrical ambiguity of the array rather than a second physical emitter. The case therefore verifies the consistency between the simulated array model and the DOA estimation chain, while also illustrating the angular ambiguity of linear arrays.

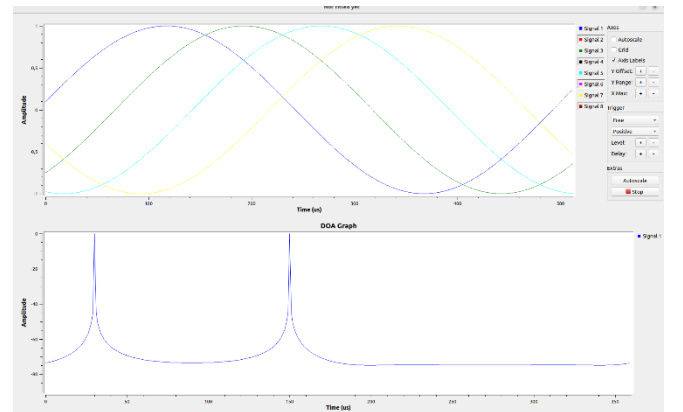


Fig. 5. MUSIC pseudo-spectrum for the reference single-source scenario at 30° .

In the two-source case, the steering matrix is extended to two columns corresponding to 30° and 80° , and the MUSIC block is configured for two sources. In an unambiguous sector, the expected result is the appearance of two distinguishable pseudo-spectrum peaks. In the full 0° – 359°

scan used for visualization, each of these directions can also produce its mirror counterpart due to the ULA geometry.

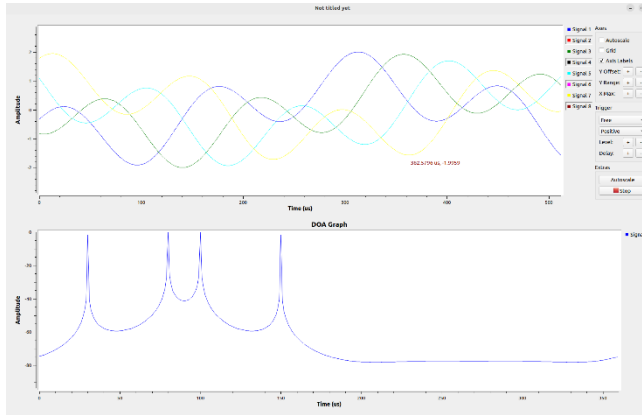


Fig. 6. MUSIC pseudo-spectrum for the two-source spatial inconsistency scenario with emitters at 30° and 80°.

From an EP perspective, the second peak may be interpreted as a spatial inconsistency when only one legitimate emitter direction is expected. This condition does not by itself prove deception or spoofing, but it provides an additional spatial indicator that can be combined with time, frequency, phase, power, and correlation consistency checks.

○ Practical implementation and coherence issues

Although the simulation demonstrates the conceptual feasibility of SDR-based spatial signal analysis, physical implementation is considerably more demanding. Practical AoA/DOA estimation, beamforming, null steering, and spatial consistency analysis require a phase-coherent multichannel receiver. This requirement is difficult to satisfy with commonly available SDR platforms, because they are typically two-channel devices. For a four-element array, a practical low-cost approach may require two USRP B210 devices operated as a combined receiver.

The initial practical configuration considered in this work uses two USRP B210 devices synchronized by an external OctoClock. The OctoClock distributes common timing and frequency references, which is a necessary step toward coherent operation. However, a common 10 MHz reference and PPS do not automatically guarantee deterministic inter-device carrier phase alignment. Even when both B210 devices are locked to the same external references, an unknown phase offset may remain between the channels belonging to different devices.

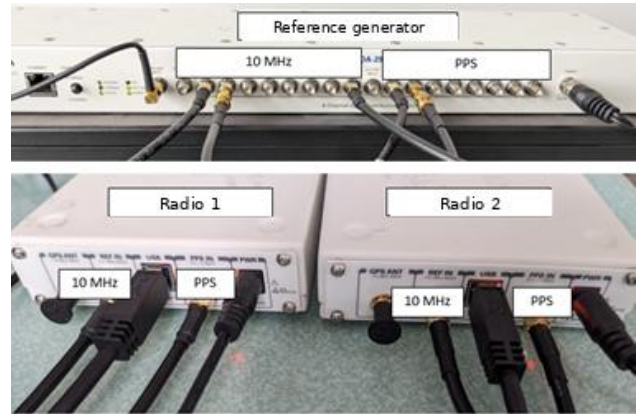


Fig. 7. Initial experimental setup for coherence establishment between two USRP B210 devices using an external OctoClock/reference generator distributing 10 MHz and PPS signals.

The residual phase ambiguity is critical for array processing because the steering model in (2) assumes known and stable inter-channel phase relationships. If the actual received channel contains an additional unknown phase term, the effective received samples can be represented as:

$$\tilde{x}_m[n] = x_m[n]e^{j\phi_m} \quad (7)$$

where ϕ_m is the residual phase offset of the m -th receiver channel. For channels located inside a single coherent SDR device, this term may be stable or easier to calibrate. For channels distributed across separate B210 devices, the inter-device component of ϕ_m may be unknown after startup, retuning, or local oscillator relocking. Therefore, external synchronization must be complemented by explicit phase calibration.

A typical digital compensation step applies an estimated calibration phase to each channel:

$$\hat{x}_m[n] = \tilde{x}_m[n]e^{-j\hat{\phi}_m} \quad (8)$$

The calibration phase $\hat{\phi}_m$ can be estimated by injecting a common reference signal, using a splitter-based calibration path, transmitting a known pilot signal from a fixed direction, or periodically estimating inter-channel phase differences during operation. Without such calibration, MUSIC peaks may be shifted, broadened, or become unstable, and subsequent beamforming or null-steering weights may be incorrect.

○ Discussion and limitations

The simulation and initial coherence considerations show that SDR can be used not only as a waveform implementation platform, but also as a platform for spatial signal analysis. The GNU Radio model demonstrates how steering-matrix-based antenna-channel generation and MUSIC-based DOA estimation can support source localization and spatial inconsistency detection. These functions are relevant to EP mechanisms such as beamforming, null steering, jammer/source localization, and anti-deception or anti-spoofing indication.

At the same time, the results should be interpreted as proof-of-concept evidence rather than as a complete operational

EP implementation. The simulation does not include RF front-end impairments, antenna mutual coupling, multipath propagation, finite ADC dynamic-range effects, synchronization errors, phase calibration drift, or coherent replay signals. In a real multichannel SDR system, these factors may significantly affect DOA accuracy and may require hardware calibration, spatial smoothing, temporal decorrelation, multi-frequency processing, and joint time-frequency-spatial consistency analysis.

Consequently, the main implementation challenge is not only the MUSIC algorithm itself, but also the establishment and preservation of phase coherence across all receiver channels. This is especially important when the required number of antenna channels exceeds the native coherent channel count of a single SDR device and multiple SDR platforms must be synchronized and calibrated as a single array receiver.

VI. CONCLUSIONS

SDR is a suitable platform for implementing a big part of EP functionality. SDR, enables implementation of adaptive waveforms, frequency agility, spread spectrum techniques, digital filtering, spectrum sensing, interference detection, modulation and coding adaptation, and algorithms for identifying spoofing or deception attempts.

Instead of this cannot implement the entire EP domain by itself. For example, several EP functions are primarily hardware-dependent or system-level in nature. Similarly, beamforming and null steering require more than software. They require different technics such as suitable antenna array, common timing and frequency references, and calibration of the RF channels.

Therefore, the most accurate statement is that SDR is a powerful and convenient implementation platform for adaptive EP, but it is not sufficient as a stand-alone solution for the full EP domain.

The GNU Radio proof-of-concept further shows that SDR can support spatial signal analysis through DOA estimation. This capability can contribute to source localization, beamforming and null steering preparation,

and spatial consistency checking for anti-deception and anti-spoofing. However, practical implementation requires a coherent multichannel receiver architecture. Initial considerations with two USRP B210 devices synchronized through an external OctoClock indicate that common timing and frequency references must be complemented by explicit inter-device phase calibration.

REFERENCES

- [1] "FM 3-12: Cyberspace operations and Electromagnetic Warfare", US Army, August, 2021. [Online]. Available: <https://irp.fas.org/doddir/army/fm3-12.pdf>
- [2] "Air Force Doctrine Publication 3-85: Electromagnetic Spectrum Operations", US Air Force, Dec. 14, 2023. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf
- [3] "AAP-06: Glossary of terms and definitions", NATO, NSO, 2021. [Online]. Available: <https://standard.di.mod.bg/pls/mstd/f?p=600:1:8391929042894131>
- [4] „Electromagnetic Warfare”, NATO, Mar. 22, 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_80906.htm
- [5] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, vol. 24, Issue: 2, pp. 767 – 809, Second quarter 2022.
- [6] "Allied Joint Doctrine for Electronic Warfare", NATO Standard AJP-3.6, March 24, 2020.
- [7] R. J. Lackey and Donald W. Upmal, "Speakeasy: The Military Software Radio", IEEE Communications Magazine, vol. 33, Issue 5, pp. 56 - 61, May 1995.
- [8] J. Mitola III, "Software Radios: Survey, critical evaluation and future directions", IEEE Aerospace and Electronic Systems Magazine, Vol. 8, Issue 4, pp. 25 – 36, April 1993.
- [9] J. Mitola III, "The Software Radio Architecture", IEEE Communications Magazine, vol. 33, Issue 5, pp. 26 - 38, May 1995.
- [10] A. Margulies and J. Mitola III, Software Defined Radios: A Technical Challenge and a Migration Strategy: IEEE 5th International Symposium on Spread Spectrum Technologies and Applications, September 2-4, 1998, Sun City, South Africa. Piscataway NJ: IEEE Service Center, 1998.
- [11] A. Wyglinski, T. Collins, D. Pu, and Robin Getz, Software-Defined Radio for Engineers. Norwood, MA, Artech House, 2018.
- [12] R. O. Schmidt, "Multiple emitter location and signal parameter estimation," IEEE Transactions on Antennas and Propagation, vol. 34, no. 3, pp. 276–280, Mar. 1986.

Assessment of EU Digital Identity Wallet from Security Perspective

Alexander Yankov

Law and History Faculty, South-West University "Neofit Rilski"

Blagoevgrad, Bulgaria

alexander.yankov1990@gmail.com

ORCID: [0009-0001-2795-0562](https://orcid.org/0009-0001-2795-0562)

Abstract — The European Union tries to introduce a sovereign digital ecosystem centered on the European Digital Identity Wallet (EUDI), a user-controlled instrument designed to combine strong technical safeguards—multi-factor authentication, zero-knowledge encryption, and secure hardware elements (SE/TEE)—with the legal mechanisms such as qualified electronic signatures (QES) under eIDAS 2.0. The wallet promises GDPR-compliant local storage of personal identification data and streamlined access to cross-border digital services, while supporting a risk-based hierarchy of Levels of Assurance (LoA) to match authentication strength to transaction sensitivity. However, the architecture and policy choices that enable these benefits also introduce significant security, privacy and socio-economic risks: key compromise and supply-chain vulnerabilities; tensions between device-centric and cloud-assisted models; potential loss of financial privacy with a digital euro; profiling and exclusion of vulnerable populations; and data minimization. Successful deployment therefore requires not only robust cryptography and certified hardware, but also resilient recovery mechanisms, interoperable standards, transparent governance, independent audits and inclusion policies that balance security, convenience and civil liberties.

Keywords — European Digital Identity Wallet, sovereign digital ecosystem, level of assurance, GDPR, digital euro.

I. INTRODUCTION

One of the new aspects of the European Union (EU) development is its efforts to shape a new digital reality based on sovereignty, security and trust. In her 2025 State of the Union address, European Commission President Ursula von der Leyen [1] presented a vision of a future in which digital sovereignty, resilience, data protection and digital identity come to the fore. These principles reflect a reality in which security, privacy and accountability would become not just regulatory requirements but competitive advantages.

The proposal for a European Digital Identity Wallet (EUDI) [2] aims to ensure security through strong multi-

factor authentication (MFA) [3], zero-disclosure encryption and secure hardware elements (SE/TEE) [4] in devices. The digital wallet is expected to meet General Data Protection Regulation (GDPR) standards [5], protecting personal data from fraud and giving users control over what information they share. The wallet will allow for the safe storage of personal documents, driving licenses and bank cards, ensuring secure access to digital services across the European Union [6]. At the same time, however, architectural and regulatory solutions create new attack possibilities and institutional risks that require in-depth analysis.

II. METHODOLOGY

The study adopts a qualitative, interpretive methodology that triangulates legal-text analysis, standards appraisal, and socio-technical risk assessment to interrogate the design and implications of the European Digital Identity Wallet. It systematically analyzes primary regulatory instruments and technical standards—most notably eIDAS 2.0, GDPR, and ISO 18013-5—treating these texts as both normative frameworks and sources of technical requirements. Complementing this close reading, the paper employs comparative evaluation to contrast device-centric and account-centric architectures (drawing on examples from commercial native wallets) and uses a risk-based analytic lens to map potential threats across technical, institutional, and social dimensions—privacy loss, exclusion, and supply-chain vulnerabilities are foregrounded. Methodological attention is also given to normative implications: the work links technical assurance levels (LoA) to legal and economic outcomes, assessing how different assurance thresholds affect accessibility and trust. In conclusion, the paper situates its findings within broader policy debates, noting that the introduction of a European Digital Identity Wallet is a serious step towards digital integration and legal digitalization in the EU.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.39>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

III. EUDI AND THE EUROPEAN SOVEREIGN DIGITAL ECOSYSTEM

Undoubtedly, the European Union is striving to invest in its own technologies, reduce dependence on external suppliers and strengthen control over cloud, hardware and information systems. Digital sovereignty is becoming not only a condition for security, but also a strategic priority on the path to long-term independence. Developing domestic capacities in areas such as cloud technologies, hardware solutions and digital infrastructure would allow Europe to innovate and function without external dependencies [7].

The European Digital Identity Wallet, currently under development, will radically change the way citizens store and share personal information [8]. Legal entities also will need to adapt to the new system, strengthening data protection and strengthening consumer trust. The General Data Protection Regulation is becoming increasingly stringent, not allowing organizations to limit themselves to formal compliance. At its core, the GDPR protects citizens' rights and maintains their trust. Encryption, least privilege access and transparent accountability reduce risks and demonstrate responsible data management. Europe's digital future depends on whether and to what extent systems and organizations can prove themselves worthy on a daily basis. But it is built on trust [9]. Companies that implement zero trust principles, protect data at all stages and build processes that are aligned with digital sovereignty will not only meet regulatory requirements – they will gain a real competitive advantage in the future. The result will be reliable digital identity protection, regulatory compliance and confidence in the EU's evolving digital requirements.

It should be noted that the EUDI wallet is a fully European solution, with its core infrastructure and identification services meeting the highest European data protection and security standards. It will offer legal entities strategic assurance that sensitive contract and customer data remains in the EU and is not exposed to access from third countries [9].

IV. DISCUSSION ABOUT THE LEVEL OF ASSURANCE AND THE DIGITAL IDENTITY

As is well known, in the digital world, identity is not a binary concept of 'known/unknown', but a spectrum of assurance. The Level of Assurance (LoA) [10] quantifies this assurance, representing the degree of conviction that the person claiming a given identity is indeed its true owner. This is the foundation of digital trust behind every secure transaction and interaction. A higher LoA means a more stringent verification and authentication process, which reduces the risk of fraud, unauthorized access and abuse. Therefore, choosing the right LoA is a critical risk management exercise that must balance security, convenience and accessibility. Therefore, for low-risk actions — such as creating a forum account or changing your address — a lower LoA is acceptable, but for high-risk transactions — accessing financial or medical data, large money transfers, signing contracts — a high LoA is required [11].

The conclusion is that LoA is not an abstract technical rating; it is the 'gateway' that defines what a user can do in the digital world. The LoA, assigned to a digital certificate or required by a service, defines the scope of transactions, the level of access, and the legal force of actions [12].

This is why the trust system and the required LoA are not only a technical but also an economic and social tool. Too high requirements can create a 'digital fortress' inaccessible to a part of the population, limiting digital inclusion. Too low standards lead to fraud, undermine trust in the digital economy and lead to so called 'digital death' [13] of the persons. This tension determines the different approaches of the world's leading economies. A system supporting multiple LoA allows for a flexible architecture tailored to risk. A certificate with a 'high' LoA can be used for services requiring a 'substantial' or a 'low' LoA, but not vice versa. This hierarchy ensures that the level of trust corresponds to the risk.

In this sense, the European Digital Identity Wallet (EUDI) is a central element of the eIDAS 2.0 Regulation [2]. It is designed as a secure, user-controlled application, provided by each Member State, that allows the storage and transmission of personal identification data (PID) [14] and electronic attributes (EAA) [15] — such as a driving license, diploma or prescription.

The abovementioned Regulation requires each Member State to provide its citizens with at least one wallet. The core architectural component is the Wallet Unit, which resides on the user's personal mobile device and relies on a local or remote Wallet Secure Cryptographic Device (WSCD) [16] for its security. This design inherently ties the wallet's highest security features to the context of a specific device. Although the ARF [17] clearly describes the flows for use across devices—for example, using a smartphone to scan a QR code to authenticate a session on a laptop—this is a model of interaction, not synchronization. True synchronization of wallet state, including its private keys and credentials, across multiple devices is technically complex and creates significant security challenges that could conflict with the eIDAS principle of 'single control' by the user [10].

A critical question in wallet architecture is whether digital credentials are tied to the user's device or to their account or the tension between device-centric security and account-centric user experience. ISO 18013-5 [18] is fundamentally device-centric in its security architecture. Its primary goal is to prevent credential cloning and ensure that credential presentation occurs from the authentic device to which the credential was issued. This is achieved through strong device affinity, in which the credential's private keys are stored in a secure, tamper-resistant hardware component of the mobile device, such as a Secure Element (SE) or Trusted Execution Environment (TEE). During presentation, the device performs a cryptographic operation with this key, proving that it is the authentic holder of the credential. The standard explicitly requires that credentials be stored either on the original mobile device or on a server

managed by the issuing authority, reinforcing this device-centric model.

However, the standard does not explicitly prohibit the use of a user account as a management and orchestration layer. This has led to the emergence of a hybrid model, particularly in the native wallet implementations of the companies such as Apple and Google. In this model, the cryptographic security anchor remains the physical device, but a user-facing cloud account (such as an Apple ID or Google Account) serves as the lifecycle management anchor. This account layer can facilitate user-friendly features, such as the migration of credentials to a new, trusted device nearby (in the case of Apple).

A key architectural question would be how the wallet would work across multiple devices. The current architecture (ARF) assumes that the EUDI would not be a typical cloud service with synchronization. Instead, the user would have one primary device — their ‘source of trust’. The basic principle in this case would be to have one primary wallet, issued by the Member State and linked to the primary device. However, this would immediately raise the question of how to proceed in cases of dual citizens of two EU Member States and whether they would be allowed to have two independent wallets.

This approach would make EUDI not a ‘cloud wallet’ but a kind of ‘identity hub’. The primary device is required for critical operations. This highlights the need for reliable backup and recovery mechanisms, as losing the device could temporarily block the digital identity.

V. QUALIFIED ELECTRONIC SIGNATURE AND CRYPTOGRAPHIC VERIFICATION

While the authentication process confirms the identity of the wallet holder, the digital signature certifies legal intent. The highest form in the EU is the qualified electronic signature (QES) [19]. According to eIDAS, it has the same legal force as a handwritten signature. A document signed with a QES cannot be rejected just because it is electronic, making QES the ‘gold standard’ for transactions.

It should be borne in mind that it is likely that the next development within the EU will be multi-wallet. Organizations should support standards such as OpenID4VP [20] and ISO 18013-5 to accept attributes from different wallets — EUDI, embedded wallets of operating systems, and others. At the same time, however, users and holders of e-wallets should be educated to trust cryptography, not the screen. Ordinary people should understand that visual verification of the screen is easy to forge and cryptographic verification is necessary.

VI. EUDI AND THE DIGITAL EURO

Last but not least, it should be noted that the claims related to the EUDI and the introduction of the digital euro. The introduction of the EUDI and the digital euro carries some significant risks, such as the loss of financial privacy. While the cash is anonymous, the digital euro could allow for the tracking of absolutely all transactions. Another very likely risk would be the profiling of citizens,

as detailed profiles of purchases, habits and location could be used for advertising or control [21]. Not without importance is the exclusion of vulnerable groups — such as people without smartphones, the elderly or people with low digital literacy, who could be excluded from the opportunity to benefit from the European digital wallet.

Next, the role of commercial banks as a kind of guarantor in a number of socio-economic processes will be undermined. They will also lose their place as an intermediary between the central banks of the member states and ordinary citizens and legal entities. When more payments go through the digital euro, banks would certainly lose their place in trade turnover. Also, it is possible to initially introduce a certain limit — for example, up to 3,000 euros per person — so that the digital euro does not turn into a complete investment instrument.

VII. BULGARIA AND EUDI

Although no official statistical data are currently available, Bulgaria is steadily progressing toward the introduction of the European Digital Identity Wallet. Expected results from the implementation of the law include the deployment of a Bulgarian European Digital Identity Wallet, expanded access to electronic services, reduced administrative burden, and enhanced security and trust in electronic interactions across the EU [22]. These expectations align with findings from studies conducted across the Union. Research by the European Commission specifically examines which potential use-cases are considered most attractive by different segments of the EU-27 population [23]. The use-cases with the highest relative importance are linked to healthcare—namely accessing health records and using electronic prescriptions—followed by electronically signing personal documents and making payments through a digital wallet. Use-cases of high relative importance are generally consistent between women and men, with the exception of accessing important documents, which women rate as highly important and men as moderately important. More pronounced differences appear across age groups: while electronic prescriptions are rated as highly important among respondents over 50, payment through a digital wallet is rated as highly important among respondents aged 18–34 and 35–49 [23].

VIII. CONCLUSION

The introduction of a European Digital Identity Wallet (EUDI) is a serious step towards digital integration and legal digitalization in the EU [24]. It combines powerful technical mechanisms (MFA, SE/TEE) with the legal force of the qualified electronic signature (QES). However, the architectural solutions — device orientation, federated model, interaction with the digital euro — give rise to risks ranging from compromise of keys and vulnerabilities in the supply chain to systemic surveillance and social exclusion. The conclusion is that success

depends not only on cryptography, but also on the quality of implementation, transparency, independent audit and recovery and inclusion policies.

REFERENCES

- [1] 2025 State of the Union Address by President von der Leyen, 10th September, 2025. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053. [Accessed: Dec. 15, 2025].
- [2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, PE/68/2023/REV/10J L, 2024/1183, 30th April 2024. [Online]. Available: ELI: <http://data.europa.eu/eli/reg/2024/1183/oj> [Accessed: Oct. 26, 2025].
- [3] (MFA) is a security process requiring users to provide two or more verification factors to gain access to an account, rather than relying solely on a password. By combining factors—something you know (password), have (smartphone), or are (biometrics)—MFA significantly reduces the risk of unauthorized access. [Online]. Available: https://trusted-digital-identity.europa.eu/eu-login-help/what-multi-factor-authentication-or-2fa_en [Accessed: Nov. 26, 2025].
- [4] Secure Elements (SE) and Trusted Execution Environments (TEE), are foundational technologies for establishing a root of trust and protecting sensitive data in modern connected devices. “Hardware Security: Understanding the Differences Between a Secure Element, TPM, HSM, and a TEE”, June, 13th 2025. [Online]. Available: <https://tropicsquare.com/blogs/hardware-security-understanding-the-differences-between-a-secure-element-tpm-hsm-and-a-tee>. [Accessed: Jan. 10, 2026].
- [5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, pp. 1–88. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>. [Accessed: Nov. 14, 2025].
- [6] S. Pabst “EU Digital Identity Wallet Pilots Roll Out Under the Radar”, October, 6th 2023. [Online]. Available: https://brownstone.org/articles/eu-digital-identity-wallet-pilots-roll-out-under-the-radar/?gl=1*u4jcp6*_gcl*_au*MTgxMzY3MDQwMS4xNzc0MTgwNjI4*_ga*MjEzMjc4NDc3MjY4Nzc0MTgwNjI4*_ga_P6T1TNYZ37*cZ3NzQxOTEyNTEkbzlkZzAkDE3NzQxOTEyNTEkajYwJGwwJGgw [Accessed March 3, 2026].
- [7] A. Tomanová “EU chystá vlastní digitální peněženku do mobilu! Kdydorazi a co všemánabídnout?”, 23.08.2025. [Online]. Available: <https://www.letemsvetemaplem.eu/2025/08/23/eu-chysta-vlastni-digitalni-penezenku-do-mobilu-kdy-dorazi-a-co-vse-ma-nabidnout/>. [Accessed Jan. 12, 2026].
- [8] “Commission Implementing Regulation (EU) 2024/2979 — integrity and core functionalities of European Digital Identity Wallets”. EUR-Lex. European Commission. 4 December 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj/eng [Accessed: Dec. 21, 2025].
- [9] A. Kwiatkowska “Europe 2025: How Organisations Can Protect Data and Identity at Scale”, 31 October 2025. [Online]. Available: <https://www.keepersecurity.com/blog/2025/10/31/how-organisations-can-protect-data-and-identity-at-scale/> [Accessed Feb. 16, 2026].
- [10] What is a level of assurance? eIDAS Levels of Assurance. [Online]. Available: <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110081/eIDAS+Levels+of+Assurance>. [Accessed: Feb. 13, 2026].
- [11] EUDI Wallet: what are the mechanisms and guarantees of the trust model? 26 February 2025. [Online]. Available: <https://www.idakto.com/blog/eudi-wallet-what-are-the-mechanisms-and-guarantees-of-the-trust-model/>. [Accessed: Dec. 20, 2025].
- [12] N. Tsakalakis, “Analysing the impact of the GDPR on eIDAS: Supporting effective Data Protection by Design for cross-border electronic identification through unlinkability measures”, Thesis for the degree of Doctor of Philosophy, University of Southampton. 2020. [Online]. Available: https://eprints.soton.ac.uk/447268/1/N_Tsakalakis_PHD_WAIS_201120.pdf. [Accessed: Jan. 26, 2026].
- [13] Digital death refers to the management, legacy, and transformation of a person's digital footprint—social media, cloud storage, emails, and assets—after they pass away. It covers legal, ethical, and personal issues regarding who owns, controls, or deletes this data, alongside the rise of digital, AI-generated memorialization and immortality. See also S. Pitsillides, M. Waller and D. Fairfax, “Digital Death: What Role Does Digital Information Play in the Way We are (Re)Membered?”, In book: Digital Identity and Social Media, pp.75-90. July 2012. [Online]. Available: https://www.researchgate.net/publication/291811561_Digital_Death_What_Role_Does_Digital_Information_Play_in_the_Way_We_are_ReMembered [Accessed Jan. 12, 2026]. <https://doi.org/10.4018/978-1-4666-1915-9.ch006>.
- [14] Personally Identifiable Data (PID or Personal Identifiable Information - PII) is any data that can distinguish, trace, or locate an individual's identity, such as names, Social Security numbers, biometric records, or combinations of data like date of birth and address. It is used to verify identity and is heavily protected by privacy laws to prevent fraud. [Online]. Available: <https://www.ibm.com/think/topics/pii>. [Accessed: Jan. 16, 2026].
- [15] An Electronic Attestation of Attributes (EAA) is a type of digital document that confirms the accuracy of a specific attribute, such as a place of residence or professional qualification. Unlike the attribute itself, which is merely a data point, the EAA serves as an official, machine-readable document. It is issued by an authorized provider, guaranteeing authenticity and carrying the same legal value as its paper-based equivalent. An EAA can be added, stored and presented with the EU Digital Identity Wallet. [Online]. Available: <https://www.digital-identity-wallet.eu/news/what-are-the-3-types-of-electronic-attestations-of-attributes-eaa/> [Accessed: Jan. 16, 2026].
- [16] WSCD a highly secure, tamper-resistant hardware component designed to store, manage, and protect sensitive cryptographic assets like private keys, credentials, and biometric templates, specifically for digital ID wallets. See also “Is WSCD and WSCA described in European Digital Identity Wallet (EUDIW) ARF equivalent to SSCD?”. [Online]. Available: <https://www.methics.fi/is-wscd-and-wsca-equivalent-to-sscd/>. [Accessed: Feb. 22, 2026].
- [17] Architecture and Reference Framework (ARF) is a set of common standards and technical specifications and a set of common guidelines and best practices. IT is a the main narrative text that describes the European Digital Identity Wallet and its ecosystem. See also “Version 2.0 of the Architecture and Reference Framework now available”, 29th May 2025. [Online]. Available: <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/900014854/Version+2.0+of+the+Architecture+and+Reference+Framework+now+available>. [Accessed: Nov.20, 2025].
- [18] ISO 18013-5:2021 is the international standard for mobile driver's licenses (mDLs), defining secure, interoperable technology for storing and presenting driver's licenses on mobile devices. It enables contactless verification via NFC, QR codes, or Bluetooth, ensuring high-level security, data integrity, and privacy-preserving, user-controlled sharing. [Online]. Available: <https://www.iso.org/standard/69084.html>. [Accessed: Dec. 12, 2025].
- [19] Qualified electronic signature (QES) is the most secure, legally binding electronic signature under EU eIDAS regulation, equivalent to a handwritten signature. It requires strict identity verification, a qualified certificate, and a secure signature creation device (QSCD). [Online]. Available: <https://commission.europa.eu/system/files/2023-03/Instructions%20for%20QES%20signature%20of%20documents.pdf>. [Accessed: Dec. 18, 2025].
- [20] OpenID4VP is a protocol that extends the OpenID Connect standard, enabling users to securely present cryptographically verifiable credentials to prove their digital identity online without relying on passwords or traditional forms of authentication. [Online]. Available:

<https://www.corbado.com/glossary/open-id-4-vp>. [Accessed: Jan. 17, 2026].

[21] G. Belova and G. Georgieva Fake News as a Threat to National Security, International conference KNOWLEDGE-BASED ORGANIZATION, Vol. 24, Issue 1, pp. 19-22, June 2018. [Online]. Available: https://www.researchgate.net/publication/326653453_Fake_News_as_a_Threat_to_National_Security. [Accessed March 3, 2026]. <https://doi.org/10.1515/kbo-2018-0002>.

[22] T. Marinova and B. Popov Bulgaria Moves to Introduce European Digital Identity Wallet, Bill set for Public Consultation, BTA, 21.02.2026, [Online]. Available: [BTA: Bulgaria Moves to Introduce European Digital Identity Wallet, Bill Set for Public Consultation](#) Accessed: March 8, 2026].

[23] EUDI Wallet – NiScy – Comprehensive Use Cases and User Research Report DLV-03-02.01-08. [Online]. Available: [What do Europeans want out of their EUDI Wallets New study sheds light - EU Digital Identity Wallet](#) -. Accessed: March 8, 2026.

[24] A. Lozenska-Todorova, "Introduction of Digital Wallets in Bulgaria and the EU", International Politics, vol 2, 2024, pp. 91-115. A. Лозенска-Тодорова „Въвеждане на цифров портфейл в България и ЕС“, сп. „Международна политика“, бр.2, 2024, с. 91-115. [Online]. Available: <http://ip.swu.bg/mod/data/view.php?id=1&advanced=1&filter=1&paging&page=1>. [Accessed Feb. 23, 2026].

Criminalization as a Tool for Ensuring National Security in the Modern Rule of Law. (Short Logical Statement)

Lyuboslav Lyubenov
Criminal Law Department
University of Ruse "Angel Kanchev"
Ruse, Bulgaria
lvlyubenov@uni-ruse.bg
ORCID: [0009-0008-5486-8557](https://orcid.org/0009-0008-5486-8557)

Abstract— The modern rule of law state is a state of clear legal rules and justice. In such a democratic and humane state, national security is explained, regulated and protected by law as a significant social benefit. Moreover, national security is logically understood as one of the most valuable legally protected goods. National security and its protection arise directly from the law. The rule of law itself introduces rules for measuring and achieving national security, but it is also obliged to comply with these rules. Therefore, lawmaking can be presented as one of the basic methods for guaranteeing national security. And criminalization as one of the basic manifestations of criminal lawmaking.

This publication analyzes and logically traces the impact of the criminalization of acts, and not so much the differentiation of criminal liability and the optimal criminal procedure on the quality of national security. This is relevant and important to do, because through criminal lawmaking, national security can be created, protected, enhanced and managed in a subtle, direct, nuanced, effective and long-term manner in a modern constitutional state.

Criminalization is one of the most important processes in the rule of law, because it is directly related to the creation and protection of national security. This is so, because through criminalization the most dangerous acts for the existence of national security are declared crimes. Human behavior that has gone through the process of criminalization becomes a crime, the commission of which is harmful to the existence of national security and is therefore subject to criminal prosecution. Through criminal prosecution, national security is restored and expanded. Any criminalized behavior is undesirable and harmful to the peaceful existence and development of the "man-society-state" system, and should be guided, including with scientific methods and means.

Keywords— criminalisation, national security, rule of law, criminal proceedings.

I. INTRODUCTION

The modern state of law is a state of clear legal rules and justice. In such a democratic and humane state, national

security is explained, regulated and protected by law as a significant social benefit. Moreover, national security is logically understood as one of the most valuable legally protected welfare. Here, national security is understood in general, as a favorable state of protection against influences that are harmful to the balance or the very existence of the system - "man - society - state". In a state of law, laws define not only the content of the concept of security, but also the threats to security, as well as the very instruments for their interception, control and guidance. In other words, national security and its protection arise directly from law. The rule of law itself introduces rules for the measurement and achievement of national security, but it is also obliged to comply with these rules. Therefore, lawmaking can be presented as one of the basic methods for guaranteeing national security. And criminalization as one of the basic manifestations of criminal lawmaking.

Norm making is simply one of the forms of guaranteeing the inviolability of individual levels of national security by restricting their typical possible threats. It is in this regard that this publication analyzes and logically traces the influence of the criminalization of acts, not so much the differentiation of criminal liability, and the optimal criminal procedure on the quality of national security. This is relevant and important to verify, because through criminal lawmaking, national security can be created, protected, enhanced and managed in a subtle, direct, nuanced, effective and long-term manner in a modern constitutional state. It is important also to be done from educational point of view. University education, especially in masters and doctoral programs, is unthinkable without active research. The introduction of new interdisciplinary scientific disciplines, as well as the capacity of non-university research organizations to prepare young scientists, should be encouraged. Bulgaria needs to make significant efforts to change the situation in the security system by increasing the interest in research at higher education institutions, creating conditions for the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.59>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

modern generation of modern knowledge and preparing the new generation of scientists [1].

With the help of criminal lawmaking, the prohibition and prosecution of those human actions is declared that pose an immediate danger or actually damage the system of public relations, in which national security as an architecture is enclosed. Criminal laws, therefore, are crucial for national security. They recognize, mark and paralyze its potential and/or real pests! For example, harmful activities such as: terrorism, sabotage, espionage, and cybercrime. Criminal lawmaking as a dynamic and complex activity of creating separate mandatory rules of behavior in society, is a measured and objectively manifested expression of the criminal policy conducted in the rule of law. Criminal lawmaking as a process includes criminalization, differentiation and the development of the criminal procedure. Here we are talking about criminalization. It is the most important of the three legal phenomena, since the prohibition of a given very dangerous behavior in the criminal law precedes and makes sense of the development and imposition of the corresponding behavior – punishment! In this report, the issues of differentiation and criminal prosecution are addressed to a minimal extent, as this is important and necessary for a better understanding of criminalization and the fight against crime.

II. MATERIALS AND METHODS

The purpose of this report is to examine and briefly explain the relationship between criminalization as a legal process and the protection of national security in the modern state of law. To achieve this goal, the following presentation should address two tasks, which arise from the title of the report itself.

The first task - to prove that the timely and correct criminalization of acts limits the existence and impact of one of the main destroyers of national security - crime.

The second task is to reveal briefly and logically the classical role of positive criminal law as one of the components in the national security system of the rule of law state.

The significance of the report lies in the systematization and strengthening of the logical connection between scientifically established criteria for the criminalization of acts, which, if taken into account by the legislator, eliminate the risk of over-criminalization and the unjustified endangerment of citizens' freedom in the modern state.

To accomplish the above tasks, the following scientific methods were used: normative-dogmatic, logical, scientific-systemic and interdisciplinary. Through them, individual written scientific materials, state documents and normative acts, mainly directly related to the topic of the work, were studied (tested) and the exposition is made. Only after the subject of research indicated in the title has been examined, in this way and with these means, the desired practically useful conclusion could be reached that improving the development of criminalization as a separate

rule-making process will lead to an improvement in the development of the national security system in the modern rule of law state, since the developed penal provisions act protectively towards national security as a good.

III. RESULTS AND DISCUSSION

In the rule of law, "penal policy is built and developed on the basis of the theory of the causes of crime and the counter action in modern society. For this reason, its content is determined by the following basic principles: prevention of crimes; large-scale participation of society in the fight against crime; economy of criminal repression with maximum efficiency of criminal law methods and means." From here, the guiding judgment that served to build this report can be directly derived. The development of crime in legislation, and the fight against it in legal practice, including through scientific methods and means, is an effective protection of the security of: the individual, legal entities, society and state. The acts included in the criminal law are included precisely because they threaten or damage the peaceful existence and development of public relations in the state. In other words, because these acts are against the security and integrity of the republic, life, health, property, sexual integrity of the citizen, society, etc. The Criminal Code includes only the most dangerous acts for the security of the individual, society, and the state!

At the beginning of the presentation, the content of the concept of security should be specified. In this report, it is used in its widest possible and permissible meaning, not in its deeper and more precise meanings, relative to the object of security science. This is required by the subject limitation of the publication, already set out in the title. Security here does not mean a state of absolute safety, protected safety, relative safety or transformational safety [2]. **Security is apprehended more generally as a state of protection against impacts that are detrimental to the equilibrium or the very existence of the system** (person, society, state). I accept that protection is **the prevention or successful management** of already allowed internal and/or external impacts on the equilibrium of the system [2]. It is useful to add that the modern apprehension of strategic security management requires not only continuous efforts to improve the formation and implementation of security policies, but also new approaches and specific solutions to modernize the security system, thus making it adequate to the requirements of the dynamic security environment [3]. The normal (balanced) existence of the system of public relations in the rule of law leads to security and prosperity of society and the state itself. Conversely, the anomalous development of public relations arouses concern among citizens and introduces uncertainty into their daily and professional affairs. Such significantly unfavorable changes in the balance of the system "man-society-state" occur after the commission of one or more crimes. In the language of security science, criminal behavior is a risk to national security. The concept of risk can denote a certain factor (group of factors) that can manifest itself with measurable probability and threaten the balance or existence of the system. Such factors can be: processes, phenomena, conscious/unconscious human activity, or lack

of due human activity, and so on. Here we are talking precisely about undertaking "toxic" human activity for the balance of the system of public relations.

The criminalization process is one of the most important because it is directly related to the creation and protection of national security. This is because **criminalization represents the declaration of acts dangerous to the existence of national security as crimes**. The legislator's discretion is influenced by the objective properties of these acts. The marking of acts dangerous to national security "is always the result of the interaction of two factors an objective factor – the property of the acts to damage public relations in the rule of law; and a subjective factor – the state of public consciousness, and more specifically, this is the legislator's negative assessment of the relevant acts as undesirable" [4]. The criminal law collects those acts whose existence adversely affects the existence of the objective needs of the individual and society for security. As V. Kudryavtsev shares "the legislator must be guided by four criteria for criminalizing acts" [5].

First of all, **there is an urgent need** to introduce a criminal prohibition of a given human act. Nikola Filchev aptly points out that "criminal law regulates not individual excesses, but mass manifestations" [4]. This means that the prohibition of a given behavior is dictated not by its individual negative reflection on the social relations it encroaches on, but by the social danger of all such actions on these same social relations. In order to criminalize a given act, it must be widespread [4]. Therefore, the main factor here is the sufficiently high degree of social danger of a given widespread negative behavior. Criminalization is necessary only after society has exhausted all its efforts to limit the spread of certain negative manifestations with other less repressive means known to it [4].

Secondly, **the admissibility of the criminal law prohibition** [4]. This means that the prohibition of a certain behavior must be morally justified, fairly and in accordance with the principles of criminal law, the constitution and the current criminal policy in the rule of law. When developing criminal policy, the main aspects of the development of society are taken into account and a direction is given for the construction of criminal lawmaking [6]. This means that the essential for the preservation and progress of society is centered in the development of criminal laws or individual amendments to them. The content of criminal policy is expressed in the correct combination of the method of coercion with the method of persuasion [6]. In a rule of law, criminal policy has as its essence, on the one hand, strict punishment of perpetrators of serious (very dangerous) crimes, and on the other hand, limiting the scope of criminal repression [6], when it comes to crimes with a low degree of public danger, even the provision of light punishments- without deprivation of liberty. Moreover, for certain minor manifestations, exemption from criminal liability is also allowed. Instead, other coercive measures are used.

Thirdly, **the objective adjustability** of the behavior whose prohibition is sought. This means assessing whether the act that is dangerous to national security can be measured and described thoroughly in the disposition of a

given norm and linked to a specific punishment, so that the imposition of the punishment objectively leads to the possibility of correction and reeducation of the guilty perpetrators.

Fourthly, **the appropriateness of the criminal prohibition**. This means assessing the ratio between the harm and the benefit of criminalizing a given behavior [6]. If the benefit of prohibiting a given behavior is less than the harm of prohibiting it, it should not be treated in the criminal law. The harm should be sought in terms of costs, reaction of the judicial authorities, reaction of the convicted person and his relatives, the path of investigation, reflection in other normative acts, etc.

Therefore, the assessment of whether a behavior is dangerous to national security and whether it should be prohibited by a criminal law norm is complex and can only be carried out correctly after considering the aspiration to prohibit the behavior in question with each of these four criteria. Otherwise, it leads to unjustified or ineffective creation of criminal law norms that can prohibit and sanction insignificant, neutral or useful human behavior for national security.

Behavior that has undergone the process of criminalization becomes a crime. Theoretically analyzed without unnecessary details, a crime is first of all a human phenomenon, and more specifically it is an effect. An effect, in turn, is "an externally manifested human volitional act that is freed from physical and physiological coercion" [7]. A crime as an act can manifest itself in the form of action or inaction. But in both cases, a crime is a manifestation that occurs under the control of consciousness and is aimed at changes in objective reality that the will of the person-actor allows [8].

A crime is an unlawful act, which means that it itself as a behavior is prohibited from being undertaken in objective reality by a legal norm. Illegality is "an objective quality of the crime, it expresses the fact of the objectively existing contradiction of the act with the legal norm" [8]. This legal norm does not allow its commission! Nikola Dolapchiev rightly shares that "law is not only imperative, it is also, besides that, an evaluative norm" [7]. This means that law has, first of all, an evaluative function. It defines the state of affairs in objective reality that is actually valuable for the development of society. The legal norm proclaims which social state is valuable, and that it ought to occur and/or exist in reality. **In this sense, criminal law prohibits the violation of that beneficial state in which social relations ought to exist in order for a normal, peaceful and progressive life of the individual, society and state**. Thanks to criminal law, threatening or destroying the most vital social relations concerning the security of society is prosecuted and sanctioned, i.e. it can be believed that criminal law is designed to assess which behavior happens to be most dangerous for the national security and hence to prohibit it under fear of severe punishment. Crime is punishable. This means that its commission in the legal world is sanctioned by a penalty specified in the criminal law. Penalty is a previously thought-out means of self-defense of society, which reacts against the violated conditions for the security of life by crime [6]. It expresses the negative opinion of society

towards crimes as phenomena and towards their perpetrators as persons who have deviated from the usual morality. By developing the penalty and by imposing it, the aim is to re-educate the criminal and to warn him to refrain from future acts on the one hand, and warn and educate society to refrain from crimes on the other hand.

A crime is a socially dangerous act. It threatens or damages the personality, the rights of citizens, property, the established constitutional order in the rule of law state or other interests protected by the law that operates in it. It "creates an objective danger to the optimal functioning of the social system" in the rule of law state [9]. A danger that has the potential to negatively deform public life and take away security from it.

A crime is a culpable act. Guilt is "the mental attitude of the perpetrator to the public danger of his behavior and to the socially dangerous consequences that it causes. It can be intentional or reckless" [10]. The perpetrator cannot be held criminally liable for consequences for which he did not show guilt (he did not understand them and caused them culpably).

Therefore, from what has been said so far in this field, it can be assumed that the introduction of a ban on committing acts with the highest degree of public danger and the criminal prosecution of persons who have violated this ban is fundamentally important for the protection of national security. **Hence, the conclusion that through criminal lawmaking, national security is finally grasped, further developed and guaranteed as a good!** It is protected from crimes, which are one of the most threatening human deviant phenomena! In criminal law rulemaking, security can and should be postulated as a benefit, not as a service for citizens. And this is the most desirable and most valuable thing in protecting the individual, society and the state today. In support of this reasoning, it is enough to point out what Nicolay Slatinsky stated: "the distribution of the benefit is on the principle of unconditionality, of unconditional justice, i.e. everyone receives their share of it. And the distribution of the service is related to the operation of the principle of conditionality, of criterion justice" [2].

For cognitive purposes, it can be noted that another important issue for the success of the fight against crime is the creation of penalties. In other words, the issue of the differentiation of criminal liability. It can be conditionally assumed that if criminalization represents the description and prohibition of a given behavior in the criminal law, then differentiation represents the development and connection of the behavior prohibited by criminalization with a specific type and amount of punishment. The differentiation of criminal liability means the definition in the criminal law of different criminal liability for different crimes depending on the depth of their public danger (harmfulness), socio-moral tameness, and the typical properties of the personality of the criminal perpetrator [4]. Differentiation is therefore the activity of the legislator. He develops different penalties for different crimes in the criminal law in order to protect national security. The creation of an inevitable and adequate criminal liability in terms of type and amount of a crime indicates a deterrent effect for its commission in social reality.

The factual and practical connection of the criminalized behavior with the punishment provided for its commission is carried out through the application of the norms of the criminal process. The criminal process is a way of realizing the content of the substantive criminal legal relationship. When talking about the criminal process, it ought to be borne in mind that as part of state activity, it is always related to the character, tasks and organization of the state [11]. That is why the content and arrangement of the criminal procedure institutes always follow and further develop the logic of those principles, methods and forms of work that characterize the state organization at a given historical moment. Therefore, the criminal process is always bound by significant state policies. Moreover, it is an instrument for the realization of the state criminal policy. In this line of thought, the norms of the criminal process (consciously or not) express part of the state policy in the field of national security. The criminal process provides protection for national security by effectively and fairly sanctioning its violators! In a state governed by the rule of law, this should always be done through accurate, fair and justified application of clear and expertly (scientifically) confirmed legal provisions. When developing procedural norms, the legislator should find an optimal balance between the speed and quality of the criminal process on the one hand, and between public and personal interest on the other. It is also appropriate that the development of procedural norms be subordinated to the idea of procedural efficiency (the cost of the efforts expended). The optimal criminal process consists of clear legal norms that impose the possibility of achieving maximum results in a pending criminal process with minimal effort on the part of the participating subjects. This means that the criminal process should be shaped with such legal rules that, without unnecessary expenditure of people and efforts, the objective truth be revealed as well as its inclusion in the judicial acts in each case. Only in this way can speed be achieved that is not detrimental to the administration of justice, and a low frequency of procedural errors that is not at the expense of citizens' rights!

Last but not least, it is worth emphasizing that the sum of the substantive and procedural criminal legal norms developed in the rule of law forms the positive criminal law. The latter is a set of these norms. From a formal and material point of view, this set of norms is always arranged and expressed, and perfected in criminal laws [12]. As a specific set of legal norms, positive criminal law also affects in its own more general way the protection of national security. For the truth of this statement, it is sufficient to emphasize the following conception of Rumen Markov: "by prohibiting the commission of crimes under fear of punishment, the criminal law has a general educational effect on the psyche of citizens (informational) and warning-deterrent impact, in order to motivate them to refrain from crime. The general educational effect of the criminal law is based on information about the actual social essence of the acts declared as crimes. The warning-deterrent effect, in turn, is based on the fear of the punishment specified in the law and the warning that it will be imposed upon the commission of the crime [12]. Neglecting the functions of positive substantive criminal

law leads to its violation. Any violation of positive substantive criminal law is compensated by the existence of an organized criminal procedure to correct the given violation. The norms of the criminal process, by the mere fact of their existence and entry into force, guarantee national security, because they are capable of creating a conviction in every criminal perpetrator that a fair, timely and justified procedure will be organized to reveal their crime and hence expose guilt. Thus, the written criminal procedural law educates to respect the inviolability of national security under fear of inevitable, but fair and sufficiently quick punishment otherwise.

For greater comprehensiveness, it should be mentioned that the written norms of international cooperation in criminal matters also have a beneficial impact on the protection of both national security and global security. They reveal a separate form of combating international crime. Interstate legal counteraction to crime includes the harmonization of national criminal legislation (regimes) on a global scale and the definition of their applicability by location so that the individual national criminal legal regimes do not overlap in their action [13]. This ensures the effectiveness of and in the intersection of global crime by legal means. This includes procedures such as extradition, European arrest warrant, transfer of criminal cases, recognition of foreign convictions, preliminary inquiries, etc. From what has been said, it can be safely concluded that the written norms of criminal law are useful for achieving and guaranteeing national security, because they regulate behavior that is too dangerous for national security, by limiting it by declaring it criminal, and by educating people to refrain from undertaking it in objective reality, under fear of exposure and adequate sanctioning.

IV. CONCLUSION

From the study of the question stated in the title of the report, the following more important logical conclusions (connections) can be drawn.

First of all, criminal lawmaking creates positive criminal law, which as a set of legal rules, by the mere fact of its existence, protects national security as a benefit for the citizens of the rule of law. The development of crime in legislation, and the fight against it in legal practice, including through scientific methods and means, is an effective protection of the security of: the individual, legal entities, society and the state.

Secondly, criminalization as a kind of norm-setting process is particularly important for the emergence and maintenance of national security, because through it, acts dangerous to the existence of national security are identified and declared crimes;

Thirdly, any criminalized behavior is undesirable and harmful to the peaceful existence and development of the "man-society-state" system.

Fourth, based on strict criteria, only those human actions are criminalized, the undertaking of which is contrary to security or the fair distribution of material and intangible goods that are essential for the rule of law.

Fifth, in the criminal law, each criminalized act is subject to a sufficiently deterrent, appropriate in type and amount, punishment.

Sixth, the restoration of national security violated by a single crime is achieved through the application of the norms of criminal procedure.

Seventh, the norms of criminal procedure can lead to the restoration and expansion of national security only if they have a consistent content that economically takes into account the needs of public and private procedural interests equally well. Otherwise, the criminal procedure turns from a guarantor into an obstacle to the functioning of the national security system.

REFERENCES

- [1] S. Stoykov; V. Dimitrova; Scientific Research in the Field of Security - Problems and Solutions, International Conference on High Technology for Sustainable Development Hitech 2018 Proceedings Open source preview, 2018, <https://doi.org/10.1109/HiTech.2018.8566275>
- [2] N. Slatinsky, Risk: the new name for security. Sofia: Publishing House "East-West", 2019, pp.378-384.
- [3] S. Stoykov, Risk management as a strategic management element in the security system, International Conference him/her Creative Business for Smart and Sustainable Growth, CreBUS 2019, March 2019, Article number 8840098, Category number CFP19U17-ART; Code 152084, ISBN: 978-172813467-3, <https://doi.org/10.1109/CREBUS.2019.8840098>
- [4] N. Filchev, Theoretical foundations of criminal lawmaking. Sofia: Ciela, 2005. pp. 40 – 95.
- [5] V. Kudryavtsev, Legal behavior: norm and pathology. Moscow, 1982, pp. 267-273.
- [6] D. Mihaylov, Problems of Criminal Law: General Part. Sofia: Ciela, 2007, pp. 640-642.
- [7] N. Dolapchiev, Criminal Law. Sofia: Bulgarian Academy of Sciences, 1994, pp. 167-202.
- [8] I. Nenov, Criminal Law of the Republic of Bulgaria - common part. Sofia: Sofi – R. 1992, pp.50-53.
- [9] R. Markov, Criminal Law of the Republic of Bulgaria : general part. Sofia: Ciela, 2024, pp.195.
- [10] A. Gerginov, Criminal Law of the Republic of Bulgaria. Sofia: Sofi-R, 2009, pp. 170-171.
- [11] S. Pavlov, Criminal Process of the Republic of Bulgaria : general part. Sofia: Sibi, 1996, pp. 32.
- [12] S. Balamezov, Constitutional Law : Part Two. Sofia: Sofi-R, 1993, pp.14.
- [13] A. Gerginov, International Legal Assistance in Criminal Cases. Sofia: Sofi – R, 2012, pp.9.

Integrating Green Building into National Defense Systems

Kiril Luchkov

Department of Economics, Industrial
Engineering and Management
Technical University of Sofia
Sofia, Bulgaria
kiril.luchkov@tu-sofia.bg

Mihail Chipriyanov

Department of Strategic Planning
Tsenov Academy of Economics
Svishtov, Bulgaria
m.chipriyanov@uni-svishtov.bg

Galina Chipriyanova

Department of Accounting
Tsenov Academy of Economics
Svishtov, Bulgaria
g.chipriyanova@uni-svishtov.bg

Nadezhda Veselinova

Department of Strategic Planning
Tsenov Academy of Economics
Svishtov, Bulgaria
n.veselinova@uni-svishtov.bg

Tihomir Panov

Department of Strategic Planning
Tsenov Academy of Economics
Svishtov, Bulgaria
tihomir_panov@abv.bg

Abstract — In the context of the dynamic security environment, the transition to energy independence of military infrastructure is becoming a strategic priority. However, the modernization of military facilities faces a critical conflict between traditional construction requirements for physical protection and modern sustainability standards. The study proposes a methodology for tracking the long-term effects of “green” solutions on the operational readiness of defense systems. The study contributes to the development of a strategic framework for sustainable decision-making in the defense sector. The results provide guidance for strategic planners and policymakers, arguing that the integration of sustainable technologies is essential for maintaining combat readiness in an environment with limited resources and high threat levels.

Keywords — energy autonomy, defense infrastructure, strategic planning, sustainable development.

I. INTRODUCTION

In today’s dynamic security environment, critical infrastructure is emerging as a fundamental pillar of national defense, determining both operational capacity and long-term sustainability of state systems [1]. Against the backdrop of the global energy transition, military organizations are faced with the need to adapt their facilities to environmental sustainability standards without compromising their core mission of ensuring security [6] – [7]. Despite the growing importance of this process, there is a serious deficit in the theoretical and practical understanding of “green” construction in the context of the defense sector [8].

The analysis of existing research approaches reveals a significant gap between standard energy efficiency models and the specific requirements of military infrastructure [2]. Similar challenges related to resilient, adaptive and uninterrupted power supply systems have also been identified in smart urban infrastructures, where energy continuity is essential for critical public functions [28]. Traditional frameworks, developed primarily for civilian sites, often ignore critical parameters such as the need for specific physical protection, cyber resilience of energy networks, and the requirements for full autonomy in critical situations [4] – [5]. It is this discrepancy that creates a serious obstacle to the effective implementation of modern environmental standards, since their implementation by mechanically copying civilian practices carries a risk to operational readiness [9].

This study aims to bridge this conceptual gap by developing an integrated approach to align security objectives with sustainable construction principles [10]. The main task focuses on defining a decision-making model that balances the requirements for a high level of protection with the need to optimize the environmental footprint [11]. Comparable management approaches have been explored in emergency response environments, where algorithmic coordination models are used to improve decision speed, resource deployment and operational effectiveness under high uncertainty [26]. Comparable sustainability governance challenges have been studied in corporate environments, where information systems are required to monitor environmental performance,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.161>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

accountability and reporting processes [27]. By examining the complex interdependencies between infrastructure sustainability and military capability, the study offers strategic planning guidelines that transform green investments into a real strategic asset, rather than simply complying with environmental regulations [12].

The conceptual evolution of military infrastructure reflects fundamental transformations in contemporary national defense strategy [13]. Historically, military facilities have been designed as static, centralized objects whose primary function was to concentrate resources and personnel in areas with a high degree of physical protection [14]. However, with the development of modern technologies, the focus has gradually shifted from static resilience to dynamic adaptability and operational autonomy [3]. Contemporary scientific literature emphasizes that the future of defense systems lies in the transition to intelligent, energy-independent facilities that are capable of functioning in interrupted supply chains [15]. This transformation process places new emphasis on the need to design bases that not only serve as operational centers, but also function as self-sufficient ecosystems capable of ensuring the continuity of vital processes in conditions of intense conflict [16].

In the context of energy efficiency, international standards for sustainable construction such as LEED (Leadership in Energy and Environmental Design) and BREEAM (Building Research Establishment Environmental Assessment Method) occupy a central place in the construction industry [17]. These methodologies have proven their effectiveness in reducing the carbon footprint and optimizing operating costs in the civilian sector [18]. However, a critical analysis of the existing literature reveals serious limitations in their direct application in the defense sector [19]. Military facilities operate in an environment that requires specific levels of cybersecurity, resistance to targeted impacts and the capacity to operate under information blackout conditions, parameters that are often absent or insufficiently represented in civilian certification systems [20]. Similar risk-based approaches have been applied in the management of electrical distribution assets, where infrastructure reliability under uncertainty is a primary objective [25]. Moreover, the strict requirements for operational confidentiality and the specific construction materials needed to protect critical assets often come into direct conflict with some of the “green” recommendations for open architectural spaces or specific ventilation systems set out in LEED and BREEAM [21]. Therefore, the existing scientific base highlights the need for an adapted framework (Figure 1) that integrates sustainable construction principles into the specific operational paradigms of national defense, without compromising protection and reliability requirements [22]. The conceptual framework of the study is presented in Figure 1. Specific requirements of military infrastructure (physical protection, cybersecurity, autonomy) are reflected. Civilian sustainability standards (LEED, BREEAM), which conflict with traditional requirements, are also visualized. The bridge presents the developed three-stage methodology - modified Delphi, Best-Worst Method and Cook model

with Monte Carlo, which generates 6 economic criteria with weights (C1-C6, Tables 1 and 2) and 4 security scenarios (S1-S4, Table 5). The lower part summarizes the results: the hybrid alternative A2 dominates in crisis (S2) and local conflict (S3), while Net-Zero (A3) is only positive in complete disruption (S4).

II. MATERIALS AND METHODS

To achieve the goal of this study - integrating green building principles into national defense systems through economically sound solutions - a three-stage methodology (Figure 2) based exclusively on expert assessments has been developed. The choice of this approach is dictated by the specific features of the military sector: the lack of long-term market data on the costs and benefits of green technologies in defense facilities, the high degree of uncertainty associated with future security scenarios, as well as the need to take into account qualitative criteria such as “combat readiness” and “logistical vulnerability” [1].

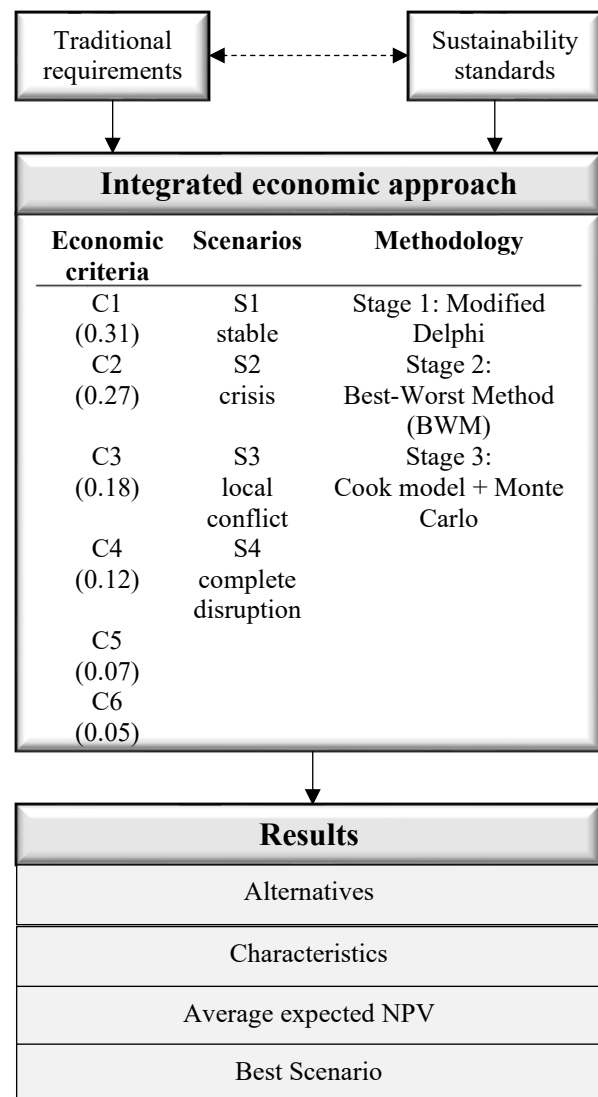


Fig. 1. Conceptual framework for integrating green building into national defense systems - conflict of requirements and bridge via economic criteria (Source: authors' own research).

A. Stage 1: Modified Delphi Method

The modified Delphi method, whose foundations were laid at the RAND Corporation [14], was applied to structure the economic criteria for evaluating green measures at a military base. The method proceeds through three anonymous rounds of surveying, with the interquartile range serving as a quantitative measure of consensus [15]. In the first round, experts freely indicate the criteria and technologies. In the second round, they rate each criterion on a Likert scale from 1 to 5. In the third round, criteria with an interquartile range (IQR) above 0.7 are returned for re-evaluation. Consensus is calculated as (1):

$$Consensus_j = 1 - \frac{IQR_j}{Q_{3j} - Q_{1j}} \quad (1)$$

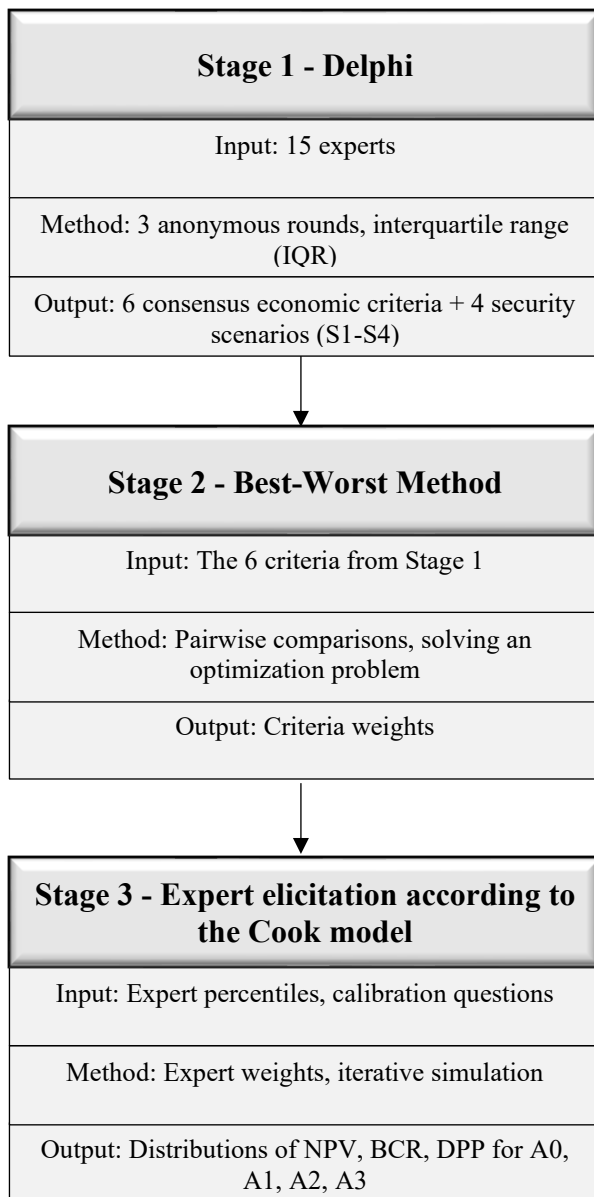


Fig. 2. Integrated methodology based on expert assessments for the defense sector (Source: authors' own research).

and is accepted at a value ≥ 0.7 . This approach has been proven to be reliable in the absence of empirical data [17]. The result of the stage is a list of 6 economic criteria and four security scenarios (stable environment, crisis, local conflict, complete disruption of supplies).

B. Stage 2: Best-Worst Method (BWM)

The Best-Worst Method (BWM) developed by Rezaei [18] was used to determine the weights of the criteria. BWM requires significantly fewer comparisons than AHP and leads to higher consistency [19]. Each expert selects the most important and least important criterion, then rates their preferences on a scale of 1-9. By solving the optimization problem (2):

$$\begin{aligned} \min \quad & \xi \quad (2) \\ \text{under condition:} \quad & \left| \frac{w_B}{w_j} - a_{Bj} \right| \leq \xi, \quad \forall j \\ & \left| \frac{w_B}{w_W} - a_{jW} \right| \leq \xi, \quad \forall j \\ & \sum_{j=1}^n w_j = 1, w_j \geq 0 \end{aligned}$$

the weights are obtained w_j . Consistency is checked by the CR coefficient, assuming $CR < 0.1$ [20]. Group weights are aggregated by the geometric mean of the individual ratings.

C. Stage 3: Expert elicitation according to the Cook model

Since many parameters (probability of PV failure in an explosion, additional maintenance costs, savings from reducing convoys) cannot be found in the literature, the classic Cook model for expert elicitation [16] is applied. The model is based on objective calibration of experts [23]. Each expert provides the 5th, 50th and 95th percentiles for 10 parameters, as well as answers to 2–3 seed questions, the correct values of which are known to the researchers. For each expert k , calibrations are calculated Cal_k and informativeness Inf_k , and its weight is (3):

$$w_k = \frac{Cal_k \times Inf_k}{\sum_{i=1}^K Cal_i \times Inf_i} \pi r^2 \quad (3)$$

The final distribution of the parameter θ is a mixture of the individual distributions: $f(\theta) = \sum_{k=1}^K w_k f_k(\theta)$. This approach has been successfully applied in engineering and risk analyses. [24].

Monte Carlo Simulation and Economic Model

With the weights and distributions obtained, a Monte Carlo simulation is performed with 1,000 iterations for each alternative (baseline, energy efficiency, hybrid, net-zero) [22]. In each iteration, the net present value (NPV) is calculated (4):

$$NPV = \sum_{t=0}^T \frac{B_t - C_t}{(1+r)^t} \quad (4)$$

where $T = 30$ years, r - discount rate, B_t - benefits (savings of energy, water, fuel, reduced logistical risk), C_t - costs (investment, maintenance, operational). Additionally, the benefit-cost ratio (BCR) and the discounted payback period (DPP) are calculated [21].

Validation is performed by cross-validation of the expert panel (division into two groups, correlation requirement $r > 0.85$ [8]. The permissible deviation is up to 30%.

III. RESULTS AND DISCUSSION

This section presents the results of the three-stage methodology. The expert panel consists of 15 people. Analyses were performed using 1,000 iterations of the Monte Carlo simulation.

A. Results of the Delphi method

After three rounds of the modified Delphi method, consensus was reached ($\text{Consensus}_j \geq 0.70$) for 6 economic criteria, which are presented in Table 1. The criteria are ranked by the median importance score on the 5-point scale.

TABLE 1 CONSENSUS ECONOMIC CRITERIA

Code	Criterion	Median (1–5)	Consensus $_j$
C1	Investment costs (€/m ²)	5.0	0.92
C2	Annual energy savings (€/year)	4.8	0.88
C3	Reduction of logistics convoys (number/year)	4.5	0.85
C4	Annual maintenance costs (€/year)	4.2	0.79
C5	Water savings (€/year)	3.9	0.74
C6	Payback period (years)	3.7	0.71

Source: Authors' own research.

Criteria C1 (investment costs) and C2 (energy savings) receive the highest consensus, confirming that economic efficiency is a top priority in the military sector. The four security scenarios are defined as follows:

S1 (Stable Environment): Normal fuel prices, low risk to convoys.

S2 (Crisis): Fuel prices +50%, moderate risk.

S3 (Local Conflict): Prices +100%, high risk, partial supply disruption.

S4 (Complete disruption): Lack of external fuel and electricity supplies for ≥ 14 days.

B. BWM Results

After applying the Best-Worst Method, the group weights of the six criteria were calculated (Table 2). The value of the consistency coefficient for all experts is $CR < 0.08$, which is below the acceptable threshold of 0.1.

As can be seen, the highest weights are given to investment costs (0.31) and energy savings (0.27), reflecting the typical military focus on initial budget and operational efficiency. Interestingly, the criterion "Reduction of convoys" is given a weight of 0.18, confirming the importance of logistical vulnerability as an economic factor.

C. Results of expert elicitation using the Cook model

Table 3 presents the pooled distributions of three key uncertain parameters obtained after weighting the experts according to their calibration and informativeness. The seed questions show that the average accuracy of the experts' 90% confidence intervals is 82%, which is comparable to published values for engineering applications.

TABLE 2 CRITERIA WEIGHTS OBTAINED THROUGH BWM

Criterion	Weight (w_j)	Standard Deviation
C1 (Investment costs)	0.31	0.05
C2 (Energy savings)	0.27	0.04
C3 (Reduction of logistics convoys)	0.18	0.06
C4 (Maintenance costs)	0.12	0.03
C5 (Water savings)	0.07	0.02
C6 (Payback period)	0.05	0.02

Source: Authors' own research.

These distributions were used as input data for the Monte Carlo simulation.

D. Monte Carlo simulation

Four alternatives for a typical military base were considered:

A0 (Baseline scenario): No green measures, only conventional construction.

A1 (Energy efficiency): LED lighting, thermal insulation, energy-efficient windows.

A2 (Hybrid): A1 + photovoltaics (200 kWp) without batteries.

A3 (Net-Zero): A1 + photovoltaics (300 kWp) + batteries (500 kWh).

After 1,000 iterations, the distributions of the net present value (NPV) for each alternative at a discount rate

of $r = 5\%$ [11] and a horizon of 30 years were obtained. The results are summarized in Table 4.

The highest expected NPV is for alternative A2 (hybrid) - 2.5 million euros, but it also carries higher uncertainty (standard deviation 0.8 million euros). Alternative A1 (energy efficiency only) has the highest probability of a positive NPV (0.96) and the shortest discounted payback period (4.2 years).

E. Analysis of security scenarios

The application of the four security scenarios (S1–S4) significantly changes the economic attractiveness of the alternatives (Table 5). In a stable environment (S1), alternative A1 dominates. In a crisis and local conflict (S2, S3), alternative A2 (hybrid) gives the highest NPV thanks to the reduction of dependence on expensive and risky fuel. In a complete disruption scenario (S4), only alternative A3 (Net-Zero) provides a positive NPV, as it allows for full energy autonomy.

TABLE 3 POOLED EXPERT DISTRIBUTIONS FOR SELECTED PARAMETERS

Parameter (unit)	Distribution type	Parameters
Additional investment costs for PV + batteries (€/kWp)	Triangular	min = 1200, mode = 1800, max = 2500
Probability of PV failure in a near-miss (0–1)	Beta	$\alpha = 2.5$, $\beta = 7.5$ (average 0.25)
Diesel savings from 100 kWp PV (l/yr)	Normal	$\mu = 22\,000$, $\sigma = 4\,500$
Additional annual maintenance of green roofs (€/m ²)	Lognormal	$\mu_{\log} = 1.2$, $\sigma_{\log} = 0.4$

Source: Authors' own research.

TABLE 4 ECONOMIC INDICATORS OF THE ALTERNATIVES (MEAN VALUES $\pm$ STANDARD DEVIATION)

Alternative	Expected NPV	P (NPV > 0)	BCR	DPP (years)
A0	0 (reference)	-	-	-
A1	+1.2 $\pm$ 0.3	0.96	2.1	4.2
A2	+2.5 $\pm$ 0.8	0.89	1.8	6.5
A3	+1.8 $\pm$ 1.1	0.74	1.3	10.2

Source: Authors' own research.

TABLE 5 EXPECTED NPV (€ MILLION) OF ALTERNATIVES UNDER DIFFERENT SECURITY SCENARIOS

Scenario	A1	A2	A3
S1 (stable)	1.5	1.8	0.9
S2 (crisis)	1.2	2.6	1.8
S3 (local conflict)	0.4	3.1	2.5
S4 (complete disruption)	-0.8	0.5	2.2

Source: Authors' own research.

These results show that the hybrid alternative (energy efficiency + RES without batteries) is the most resilient in moderate crises, while Net-Zero is justified only in extreme scenarios of complete isolation.

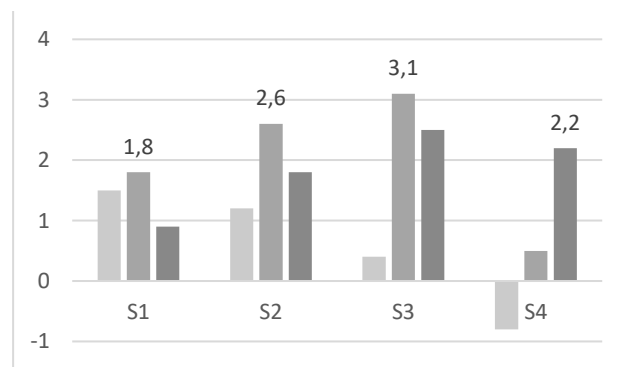


Fig. 3. Comparison of expected Net Present Value (NPV) of three green alternatives under four security scenarios (Source: authors' own research).

Figure 3 shows the expected net present value (NPV) of the three alternatives under four security scenarios. In a stable environment (S1), all three alternatives are positive, with A2 (hybrid) giving the highest NPV. In a crisis (S2) and local conflict (S3), the advantage of A2 becomes sharply pronounced. In a scenario of complete supply disruption (S4), only A3 (Net-Zero) remains positive, while A1 becomes negative. This confirms that the hybrid approach is most resilient in moderate crises, while Net-Zero is justified only in extreme isolation.

Cross-validation with the expert panel divided into two groups shows a correlation of weights $r = 0.89$ ($p < 0.001$), which exceeds the threshold of 0.85. Comparison with published data from the NATO base in Geilenkirchen shows an average deviation of expert cost estimates of 22%, which is below the permissible 30%.

IV. CONCLUSIONS

This study developed and applied a three-stage methodology based on expert assessments (modified Delphi, Best-Worst Method and Cook's model) to economically justify the integration of green building principles in defense infrastructure. The main conclusions are as follows:

a) The economic criteria with the highest priority in the military sector are investment costs and energy savings, followed by the reduction of logistics convoys (weights 0.31; 0.27; 0.18, respectively). This confirms that the focus is on budgetary efficiency and operational autonomy, and not on environmental indicators per se.

b) The hybrid alternative (energy efficiency + photovoltaics without batteries) gives the highest expected net present value (NPV = €2.5 million) and is the most resilient in crisis and local conflict scenarios. In a stable environment, energy efficiency alone (A1) is most advantageous, while Net-Zero (A3) is justified only in a scenario of complete disruption of external supplies.

c) The expert approach is confirmed as reliable in the absence of market data - cross-validation shows a correlation $r = 0.89$, and comparison with real data from a NATO base gives an average deviation of 22% (<30% acceptable).

V. OTHER RECOMMENDATIONS

Recommendations could also be made regarding green building policies in national defense systems through economically sound solutions in the following areas:

a) Military departments should introduce life cycle analysis (LCCA) when approving infrastructure projects to take into account the long-term savings from reduced fuel supplies.

b) Launch pilot projects for hybrid bases (energy efficiency + photovoltaics) in existing military facilities in temperate climates.

c) When justifying security budgets, include scenarios of complete energy disruption as an argument for investments in Net-Zero technologies.

The results obtained depend on the composition of the expert panel and do not take into account the specifics of individual geographical locations. Future research should expand the panel with international experts and verify the model using real data from implemented green systems on military bases.

VI. ACKNOWLEDGMENTS

This research was funded by the Bulgarian National Science Fund at the Ministry of Education and Science of Bulgaria under the Funding Competition for Fundamental Scientific Research Projects 2025, based on Administrative Contract № KP-06-N95/16 of 10 December 2025, for the implementation of Research Project № KP-06-PN95/45, SUNI № BG-175467353-2025-08-0248, titled „Epistemic robustness of artificial intelligence: A universal framework for evaluation in industrial and management systems“.

REFERENCES

[1] NATO Standardization Office, STANAG 7141 – Environmental Protection. Brussels: NATO, 2014.

[2] U.S. Department of Defense, *Unified Facilities Criteria (UFC) 4-010-01: DoD Minimum Antiterrorism Standards for Buildings*. Washington, DC: U.S. Department of Defense, 2018.

[3] J. D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston: McGraw-Hill, 2000.

[4] J. W. Forrester, *Industrial Dynamics*. Cambridge, MA: MIT Press, 1961.

[5] M. E. Goodsite and S. Juhola, Eds., *Green Defense Technology: Triple Net Zero Energy, Water and Waste Models and Applications*. Dordrecht: Springer, 2017.

[6] RAND Corporation, *Can NATO Supercharge Military Greening?* RAND Research Report, 2023. [Online]. Available: <https://www.rand.org/pubs/>. (Accessed: Apr. 20, 2026).

[7] K. Jeong, T. Hong, C. Ban, C. Koo, and H. S. Park, Life cycle economic and environmental assessment for establishing the optimal implementation strategy of rooftop photovoltaic system in military facility, *Journal of Cleaner Production*, vol. 104, pp. 315–327, 2015. <https://doi.org/10.1016/j.jclepro.2015.05.066>.

[8] B. Drobnič, T. Katrašnik, M. Mori, R. Šipeč, and U. Žvar Baškovič, The Energy Autonomy of Military Sites is Supported by Green Energy Hubs Including Hydrogen Technologies, NATO Science and Technology Organization, STO-MP-SAS-190, 2025.

[9] R. G. Coyle, *System Dynamics Modelling: A Practical Approach*. London: Chapman & Hall, 1996.

[10] D. H. Meadows, D. L. Meadows, J. Randers, and W. W. Behrens, *The Limits to Growth*. New York: Universe Books, 1972.

[11] G. P. Richardson, Reflections on the foundations of system dynamics, *System Dynamics Review*, vol. 27, no. 3, pp. 219–243, 2011. <https://doi.org/10.1002/sdr.462>.

[12] D. Dimitrov, *Application of scenario planning in business, defense and security*. Sofia: UNSS, 2012.

[13] U.S. Department of Defense, *Operational Energy Strategy*, Washington, DC, 2011.

[14] H. A. Linstone and M. Turoff, Eds., *The Delphi Method: Techniques and Applications*. Boston: Addison-Wesley, 2002.

[15] C. Powell, The Delphi technique: Myths and realities, *Journal of Advanced Nursing*, vol. 41, no. 4, pp. 376–382, 2003. <https://doi.org/10.1046/j.1365-2648.2003.02537.x>.

[16] R. M. Cooke, *Experts in Uncertainty: Opinion and Subjective Probability in Science*. Oxford: Oxford University Press, 1991.

[17] O. G. Manoliadis, I. E. Tsolas, and A. Nakou, Sustainable construction and drivers of change in Greece: a Delphi study, *Journal of Cleaner Production*, vol. 14, no. 18, pp. 1666–1672, 2006. <https://doi.org/10.1080/01446190500204804>.

[18] J. Rezaei, Best-worst multi-criteria decision-making method, *Omega*, vol. 53, pp. 49–57, 2015. <https://doi.org/10.1016/j.omega.2014.11.009>.

[19] J. Rezaei, Best-worst multi-criteria decision-making method: Some properties and a linear model, *Omega*, vol. 64, pp. 126–130, 2016. <https://doi.org/10.1016/j.omega.2015.12.001>.

[20] T. L. Saaty, *The Analytic Hierarchy Process*. New York: McGraw-Hill, 1980.

[21] A. E. Boardman, D. H. Greenberg, A. R. Vining, and D. L. Weimer, *Cost-Benefit Analysis: Concepts and Practice*, 5th ed. Cambridge: Cambridge University Press, 2017.

[22] R. Y. Rubinstein and D. P. Kroese, *Simulation and the Monte Carlo Method*, 3rd ed. Hoboken, NJ: John Wiley & Sons, 2016.

[23] R. M. Cooke and L. H. J. Goossens, TU Delft expert judgment data base, *Reliability Engineering & System Safety*, vol. 93, no. 5, pp. 657–674, 2008. <https://doi.org/10.1016/j.ress.2007.03.005>.

[24] A. M. Hanea and G. F. Nane, An in-depth perspective on the classical model for structured expert judgment, in *Expert Judgement in Risk and Decision Analysis*, Cham: Springer, 2021, pp. 27–56.

[25] K. Anguelov and D. Stoilov, Risk based asset management of electrical distribution network, 2016 19th International Symposium on Electrical Apparatus and Technologies (SIELA), Bourgas, Bulgaria, 2016, pp. 1–4, <https://doi.org/10.1109/SIELA.2016.7542971>.

- [26] M. Angelova and K. Anguelov, Methodology for Evaluation Effectiveness and Efficiency of Algorithmic Management in Emergency Response Teams, 2025 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1-5,
<https://doi.org/10.1109/ELMA65795.2025.11083484>.
- [27] P. Stoyanov and K. Anguelov, Corporate Social Responsibility Reporting: Information System Requirements, 2025 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5,
<https://doi.org/10.1109/COMSCI67172.2025.11225210>.
- [28] V. Zinoviev, Challenges in the Power Supply for the Needs of Smart Cities, 2019 II International Conference on High Technology for Sustainable Development (HiTech), Sofia, Bulgaria, 2019, pp. 1-4,
<https://doi.org/10.1109/HiTech48507.2019.9128268>.

Managing Environmental Risks Through ESG

Kiril Luchkov

Department of Economics, Industrial Engineering and Management
Technical University of Sofia
Sofia, Bulgaria
kiril.luchkov@tu-sofia.bg

Abstract — This study examines the potential for using Environmental, Social and Governance (ESG) as a management framework for identifying, assessing and mitigating environmental risks within an organization. Against a backdrop of increasing regulatory pressure, climate uncertainty, resource constraints and heightened corporate reporting requirements, environmental risks are increasingly becoming a strategic management issue. This study argues that ESG should not be viewed solely as a tool for non-financial reporting, but as a conceptual and practical framework through which organizations can structure their mechanisms for monitoring, prioritizing and managing environmental impacts, dependencies and vulnerabilities. On this basis, the author proposes a model in which environmental risk is viewed as the interaction of three interrelated dimensions: exposure, impact and organizational vulnerability. The model allows different environmental issues to be compared using a unified logic, prioritized and linked to differentiated management responses. The study aims to establish a clearer link between regulatory frameworks, analytical risk management, and corporate governance.

Keywords — ESG, environmental risk, risk management, sustainable development.

I. INTRODUCTION

In recent years, environmental risks have emerged as one of the most significant factors affecting the sustainability, adaptability and long-term competitiveness of organizations. Processes such as climate change, depletion of natural resources, pollution and increasing pressure on ecosystems cannot be ignored by businesses [6], [12], [13]. They should not be limited to the sphere of environmental policy. Instead, they affect the way organizations operate, including their compliance with regulatory requirements [1], [2].

The scientific literature has seen an expansion of the analysis of environmental risks beyond the climate focus. The European Sustainability Reporting Standards (ESRS) structures the environmental dimension into five distinct strands. These cover climate change, pollution, water and marine resources, biodiversity and ecosystems, as well as

resource use and the circular economy [1]. Regulatory developments related to the circular economy further reinforce the strategic importance of material efficiency, waste reduction and resource traceability [15]. In parallel, Taskforce on Nature-related Financial Disclosures (TNFD) draws attention to nature-related dependencies, impacts, risks and opportunities along the entire value chain [4], [5].

This paper is based on the understanding that environmental risk is the result of the interaction between external exposure, potential impact, and internal organizational vulnerability. At the same time, many environmental risks require investment responses, which makes access to financing mechanisms for energy-efficiency and sustainability projects an increasingly important managerial consideration [14]. The three elements are considered in their interdependence. On this basis, a conceptual framework is proposed through which ESG can be used as a means of systematizing, prioritizing and limiting environmental risks.

The focus of this study is the management of environmental risks within organizations. The subject of the study is the potential of ESG to function as a management framework for identifying, assessing and mitigating environmental risks. The aim of this study is to clarify how ESG can be used not only as a reporting tool but as a systematic management framework for dealing with environmental risks, and on this basis to propose an analytical model for their structuring and prioritization. Previous studies on corporate social responsibility reporting have also emphasized the importance of information-system requirements for collecting, processing and disclosing sustainability-related data [16].

To achieve this objective, the following tasks are set: to track the development of the academic debate on ESG and environmental risk; to identify the main areas of environmental risk relevant to organizations; to analyze the limitations of prevailing reporting and indicator approaches; to propose a conceptual framework for assessing environmental risk through the interaction between exposure, impact and vulnerability; and to

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.162>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

formulate management conclusions regarding the application of ESG in the decision-making process.

II. MATERIALS AND METHODS

Research on ESG is gradually shifting its focus from the general concept of corporate responsibility towards a more structured understanding of sustainability as a management and risk category. The early establishment of this logic was strongly influenced by the Task Force on Climate-related Financial Disclosures (TCFD) recommendations, which organize climate-related information around four key thematic areas: governance, strategy, risk management, metrics and targets [3]. Subsequently, International Financial Reporting Standard S2 (IFRS S2) further developed this framework and established it as a standard for disclosing climate-related risks and opportunities, including physical and transition risks, applicable to reporting periods beginning on or after 1 January 2024 [2], [7].

Although climate risk remains the most developed area, the newer European frameworks clearly demonstrate a broadening of the analysis beyond climate. The ESRS distinguishes the environmental dimension into five separate standards and organizes the information around management, strategy, processes related to impacts, risks and opportunities, as well as indicators and targets [1].

A similar broadening of scope is also evident in the TNFD, which is developing a framework for identifying, assessing, responding to and disclosing nature-related issues. The TNFD focuses on nature-related dependencies, impacts, risks and opportunities across the entire value chain. TNFD also proposes the LEAP (Locate, Evaluate, Assess and Prepare) approach as an integrated process for identifying interactions with the natural environment, assessing dependencies, analyzing risks, and preparing for response and reporting [4], [5].

It is precisely here that the main gap identified by this study lies. Consequently, the following sections of this paper propose an analytical framework that links regulatory standards with management practice. It should be noted that this study is of a conceptual nature. It is based on an analysis of the academic literature and regulatory frameworks.

This study employs a conceptual-analytical approach based on an analysis of the scientific literature, international ESG frameworks, and regulatory standards. A pilot test was conducted to verify the practical applicability of the proposed model. It was carried out in May 2026 at three manufacturing companies in Bulgaria operating in different industrial sectors.

III. RESULTS AND DISCUSSION

3.1. Proposed framework for managing environmental risks through ESG

In this context, this study proposes a framework according to which environmental risk should be viewed as a function of three interrelated dimensions: exposure, impact and organizational vulnerability. Exposure reflects the extent to which the organization is exposed to

environmental dependencies and impacts. It may stem from the location of assets, sector profile, raw materials used, energy intensity, water dependency, value chain sensitivity, or presence in environmentally vulnerable areas. Impact reflects the potential severity of environmental risk on the organization, including consequences for operational stability, costs, supply chains, legal compliance, reputation, access to finance and strategic sustainability. Organizational vulnerability, in turn, is the extent to which the organization is internally unprepared to identify, bear, manage and mitigate environmental risk.

For the purposes of this study, the following analytical framework is proposed:

$$\text{Environmental risk} = \text{Exposure} \times \text{Impact} \times \text{Organizational vulnerability}$$

The main elements of the model are summarized in Table 1. They are presented there together with their content and the corresponding management issues.

TABLE 1 PROPOSED MODEL FOR MANAGING ENVIRONMENTAL RISKS THROUGH ESG

Component	Content	Indicative management questions
Exposure	Degree of exposure to environmental dependencies and impacts.	Where is the organization most dependent on natural resources? Which assets, processes or parts of the value chain are most sensitive?
Impact	Potential severity of the consequences on operations, financial position and strategy.	What might be the impact on costs, operations, access to capital, regulatory compliance and reputation?
Organizational vulnerability	Internal unpreparedness to identify, manage and mitigate risk.	Are there reliable data, clear responsibilities, control mechanisms, scenarios and response capacity?

Source: Author's own research.

The logic behind this formula is that the three elements do not operate in isolation, but reinforce one another. Low exposure combined with high vulnerability may result in a manageable risk, but high exposure, combined with high impact and high vulnerability, leads to a significantly more severe risk profile. The advantage of such a model is that it allows for the construction of a clearer risk matrix, in which the organization is not limited to presenting its environmental issues, but prioritizes them according to their managerial significance.

For the practical application of the model, a five-point scale can be used, in which each of the three factors is rated from 1 to 5. This allows for the creation of an internal risk classification: low, moderate, high, very high and critical

risk. Such a scale should not be regarded as a universal regulatory standard, but rather as an internal management tool for comparison, prioritization and action planning.

3.2. Typology of environmental risks in the ESG framework

The application of the proposed model requires a clear distinction between the main environmental areas in which the risk manifests itself. The most logical basis for such a typology is found in the ESRS, where the environmental dimension is structured into five separate standards: climate change, pollution, water and marine resources, biodiversity and ecosystems, as well as resource use and the circular economy [1].

IFRS S2 distinguishes two main categories of climate-related risks: physical risks and transition risks. Physical risks are related to extreme weather events, prolonged climate changes, disruption of production and logistics processes, damage to assets and higher operational volatility. Transitional risks, on the other hand, arise in connection with regulatory changes, technological shifts, market expectations, investor pressure and the transformation of consumer preferences in the context of the transition to a low-carbon economy [2].

Risks related to pollution constitute a distinct category and should not be viewed as a secondary consequence of climate risk. They include air emissions, soil contamination, waste generation, hazardous substances, industrial accidents and the accumulation of environmental liabilities. Their impact is not only manifested through environmental damage. At the same time, secondary consequences are also observed, including sanctions, legal claims, business interruption, loss of trust and additional compliance costs [1].

Risks related to water and marine resources are particularly significant for industries with high water dependence. They may result from location in areas with water stress, intensive use of water resources or water

quality sensitivity. Their impact is manifested through production disruption, increased costs, stakeholder conflicts and regulatory pressures. The TNFD LEAP approach is particularly useful here because it guides the organization to identify effects on nature, assess dependencies and impacts, and only then to conduct a proper risk assessment [5].

Risks related to biodiversity and ecosystems are among the most complex to analyze [8]. They often do not manifest themselves immediately in financial and operational indicators. Nevertheless, over time they can significantly undermine the resilience of the business model.

The next area covers risks related to resource use and the circular economy. Here, exposure arises from dependence on primary raw materials, high waste streams and inefficient use of resources. The impact is expressed in higher costs, sensitivity to price changes, supply chain problems, loss of competitiveness and increased regulatory pressure. Vulnerability exists when an organization does not have sufficient traceability of material flows. It also manifests itself in the absence of circular business solutions and in the absence of measurement in terms of resource efficiency [1].

Climate risks, pollution, water stress, biodiversity loss and resource inefficiency are often intertwined and mutually reinforcing. These factors rarely operate in isolation. Therefore, the typology should serve not to mechanically categorize the topics into sections, but to build a matrix of priorities. It is precisely here that the three-factor model gains real value, because it allows the organization to compare different environmental risks according to a single principle.

In accordance with the logic outlined above, environmental risks can be systematized as presented in Table 2.

TABLE 2. TYPOLOGY OF ENVIRONMENTAL RISKS WITHIN THE ESG FRAMEWORK

Category	Typical sources of exposure	Potential impacts	Common manifestations of organizational vulnerability
Climate risks	Energy intensity, physical assets, sensitive locations, carbon footprint	Asset damage, business interruption, incidental costs, capital shortfall	Lack of scenarios, poor integration into risk management, limited data
Pollution	Hazardous substances, emissions, waste, incident risk	Fines, legal disputes, reputational damage, compliance costs	Inadequate control of flows, poor traceability, weak monitoring
Water and marine resources	Water-intensive processes, water-stressed areas, dependence on water quality and quantity	Production disruptions, higher costs, tension with stakeholders	Lack of efficiency plans and alternative sources, poor data
Biodiversity and ecosystems	Locations or suppliers in sensitive areas, dependence on functioning ecosystems	Supply chain risk, public pressure, regulatory restrictions	Lack of geographical analysis and expertise, low traceability along the supply chain
Resources and the circular economy	Material intensity, waste streams, dependence on primary raw materials	Price fluctuations, inefficiency, loss of competitiveness	Limited traceability, absence of circular solutions, poor performance

Source: Author's own research.

3.3. Application of the ESG model in environmental risk management

Within the proposed model, ESG is viewed not only as a tool for disclosure but also as a framework for management action [10]. IFRS S2 requires organizations to disclose information on the management, control and monitoring processes used, the strategy for managing climate-related risks and opportunities, the processes for identifying, assessing, prioritizing and monitoring them, as well as performance against relevant indicators and targets [2].

The practical application of the model requires a clear division of responsibilities. The governing body should have a clearly defined oversight function with regard to environmental risks, while senior management should have specific responsibilities for assessment, coordination and response [11]. Internal functions relating to risk, sustainability, finance, operations and legal compliance must be integrated into a single mechanism, rather than operating in a fragmented manner. It is precisely here that organizational vulnerability takes on a particularly managerial dimension: it measures not only weaknesses in processes, but also deficits in institutional coordination [4].

Environmental risk should not be treated as a separate issue, detached from the overall risk management framework. IFRS S2 requires organizations to disclose whether and how the processes for identifying, assessing, prioritizing and monitoring climate-related risks and opportunities are integrated into the overall risk management process. The TNFD applies much the same logic to nature-related risks [2], [4].

The effective application of the model is impossible without a reliable system of data, indicators and targets [9]. Similar data-driven approaches, including artificial intelligence applications in digital energy systems, demonstrate how environmental indicators can be continuously monitored and integrated into managerial decision-making [17]. Sustainability frameworks require organizations to disclose the indicators used to assess and manage material risks and opportunities, as well as progress towards set targets. It follows, therefore, that environmental risk management must be viewed not only as an assessment process, but also as a process of systematic measurement and internal control. In the absence of reliable data, traceability or verification procedures, organizational vulnerability remains high even when the exposure itself is not at its maximum.

Current frameworks also clearly demonstrate that environmental risk cannot be assessed solely within the confines of an organization's direct operations. The TNFD requires that dependencies, impacts, risks and opportunities be analyzed not only within direct operations but also across upstream and downstream value chains. This means that the proposed model should be applied not only at the corporate level, but also across individual business units, assets, geographical locations and key parts of the value chain [4], [5].

Where the risk assessment indicates a low risk, the focus may be on monitoring, periodic checks and limited corrective actions. Where the risk is moderate, clearer policies, internal responsibilities, indicators and routine monitoring are required. In the case of high risk, specific action plans, stricter controls, better coordination with suppliers and more active management involvement are required. In the case of critical risk, the organization must be prepared for structural changes to processes, assets, resource sources, technological solutions and strategic priorities.

The advantage of the proposed model lies in its flexibility. It can be used both in large organizations with formalized risk management systems and in more limited organizational contexts where a fully developed ESG infrastructure is lacking. At the same time, its strength lies primarily in its analytical and managerial aspects. It does not eliminate the problem of input data quality and does not claim to be a universal metric, but it creates a structured framework for assessment and response, suitable for internal management use.

3.4. Pilot Testing of the Proposed Model

To verify the practical applicability of the proposed model, a pilot test was conducted at three manufacturing companies in Bulgaria operating in different industrial sectors. The companies included in the sample have different profiles in terms of environmental exposure, resource dependence, and organizational complexity. The assessment was carried out through expert assessment on a five-point scale, in which the components of exposure, impact, and organizational vulnerability are rated on a scale of 1 to 5. The final risk score is calculated by multiplying the three components. The following factors were taken into account when determining the ratings: the company's industry profile, degree of resource and energy dependence, nature of environmental impacts, applicable regulatory requirements, and organizational mechanisms for environmental risk management and control.

In accordance with the logic outlined above, the main environmental risk areas for each of the companies have been identified. The results are presented in Table 3.

TABLE 3. PILOT TESTING OF THE PROPOSED ESG MODEL

Company profile	Main risk area	Exposure	Impact	Organizational vulnerability	Overall risk score
Food industry company with water-intensive production processes	Water resources and resource dependence	4	4	3	48
High energy-intensive mechanical engineering company	Climate and resource risks	4	3	3	36
A chemical industry company working with hazardous substances	Pollution and hazardous substances	5	5	3	75

Source: Author's own research.

The results clearly show distinct differences in risk profiles among the analyzed companies. For the food and beverage company, risks related to water resources and the dependence of production processes on constant access to water predominate. This results in a relatively high risk score. In the machine-building company, a more moderate risk profile is observed. It is mainly determined by the high energy intensity, dependence on raw materials and sensitivity to transitional climate policies and regulatory requirements. The highest risk score was recorded for the company in the chemical industry. This is due to high exposure to pollution, the handling of hazardous substances, and heightened regulatory requirements at the sectoral level. The pilot testing conducted shows that the proposed model allows for the comparative assessment and prioritization of environmental risks in companies with different sectoral profiles and organizational characteristics.

IV. CONCLUSIONS

This study is based on the understanding that environmental risks can no longer be regarded as a peripheral aspect of corporate sustainability. They should be viewed as an integral part of strategic and operational management.

The main conclusion of the study is that ESG is most valuable not when used solely as a reporting tool, but when it becomes a framework for managerial action. It is precisely in this context that the author proposes a model

in which environmental risk is viewed as the interaction of three interrelated dimensions: exposure, impact and organizational vulnerability. The advantage of this approach is that it allows different environmental issues to be compared using a consistent logic, prioritized, and linked to differentiated management responses.

The scientific contribution of this study can be summarized in three areas:

- Environmental risk is examined in the context of ESG, beyond a narrow focus on climate.
- A conceptual framework is proposed that links reporting standards to the organization's internal management logic.
- An analytical model is developed that can assist in identifying, assessing, and prioritizing environmental risks in various organizational contexts.

The proposed model is conceptual and aims to provide analytical and managerial clarity; it does not claim to be a comprehensive, universal metric that can be applied across all sectors without adaptation. Furthermore, its added value will depend on the quality of the input data, the maturity of internal processes and the organization's ability to work with spatial, chain and scenario dependencies.

The pilot testing of the model does not claim to be statistically representative or to constitute expanded sector-specific testing. Therefore, future research could focus on expanded sector-specific testing of the model in specific industries, the development of sector-specific indicators for assessing exposure, impact, and vulnerability, and a more in-depth analysis of the relationship between environmental risk, ESG reporting, and actual management decisions. The most significant conclusion, however, remains the following: the true value of ESG lies not in disclosure itself, but in its ability to structure managerial thinking and translate complex environmental interdependencies into well-reasoned decisions.

V. ACKNOWLEDGMENTS

This research was funded by the Bulgarian National Science Fund at the Ministry of Education and Science of Bulgaria under the Funding Competition for Fundamental Scientific Research Projects 2025, based on Administrative Contract № KP-06-N95/16 of 10 December 2025, for the implementation of Research Project № KP-06-PN95/45, SUNI № BG-175467353-2025-08-0248, titled „Epistemic robustness of artificial intelligence: A universal framework for evaluation in industrial and management systems“.

REFERENCES

- [1] European Commission, Commission Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU as regards sustainability reporting standards, Official Journal of the European Union, 22 December 2023, Available at: http://data.europa.eu/eli/reg_del/2023/2772/oj.
- [2] IFRS Foundation. (2023). IFRS S2 Climate-related Disclosures. International Sustainability Standards Board. Available at:

- <https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s2-climate-related-disclosures/>
- [3] Task Force on Climate-related Financial Disclosures. (2017). Recommendations of the Task Force on Climate-related Financial Disclosures. Financial Stability Board. Available at: <https://www.fsb.org/2017/06/recommendations-of-the-task-force-on-climate-related-financial-disclosures-2/>.
- [4] Taskforce on Nature-related Financial Disclosures. (2023). Recommendations of the Taskforce on Nature-related Financial Disclosures. Available at: <https://tnfd.global/publication/recommendations-of-the-taskforce-on-nature-related-financial-disclosures/>
- [5] Taskforce on Nature-related Financial Disclosures, Guidance on the identification and assessment of nature-related issues: The LEAP approach (Version 1.1), TNFD, 2023, Available at: https://tnfd.global/wp-content/uploads/2023/08/Guidance_on_the_identification_and_assessment_of_nature-related_Issues_The_TNFD_LEAP_approach_V1.1_October2023.pdf.
- [6] G. Friede, T. Busch, A. Bassen, ESG and financial performance: aggregated evidence from more than 2000 empirical studies, *Journal of Sustainable Finance & Investment*, Volume 5, Issue 4, 2015, pp. 210–233, ISSN 2043-0795, <https://doi.org/10.1080/20430795.2015.1118917>.
- [7] P. Bolton, M. Kacperczyk, Do investors care about carbon risk?, *Journal of Financial Economics*, Volume 142, Issue 2, 2021, pp. 517–549, ISSN 0304-405X, <https://doi.org/10.1016/j.jfineco.2021.05.008>.
- [8] R. Albuquerque, Y. Koskinen, S. Yang, C. Zhang, Resiliency of environmental and social stocks: An analysis of the exogenous COVID-19 market crash, *The Review of Corporate Finance Studies*, Volume 9, Issue 3, 2020, pp. 593–621, ISSN 2046-9128, <https://doi.org/10.1093/rcfs/cfaa011>.
- [9] C. Flammer, Corporate green bonds, *Journal of Financial Economics*, Volume 142, Issue 2, 2021, pp. 499–516, ISSN 0304-405X, <https://doi.org/10.1016/j.jfineco.2021.01.010>.
- [10] P. Krüger, Corporate goodness and shareholder wealth, *Journal of Financial Economics*, Volume 115, Issue 2, 2015, pp. 304–329, ISSN 0304-405X, <https://doi.org/10.1016/j.jfineco.2014.09.008>.
- [11] K. V. Lins, H. Servaes, A. Tamayo, Social capital, trust, and firm performance: The value of corporate social responsibility during the financial crisis, *The Journal of Finance*, Volume 72, Issue 4, 2017, pp. 1785–1824, ISSN 0022-1082, <https://doi.org/10.1111/jofi.12505>.
- [12] P. Bansal, M. R. DesJardine, Business sustainability: It is about time, *Strategic Organization*, Volume 12, Issue 1, 2014, pp. 70–78, ISSN 1476-1270, <https://doi.org/10.1177/1476127013520265>.
- [13] R. Sassen, A. K. Hinze, I. Hardeck, Impact of ESG factors on firm risk, *Journal of Business Economics*, Volume 86, Issue 8, 2016, pp. 867–904, ISSN 0044-2372, <https://doi.org/10.1007/s11573-016-0815-2>.
- [14] K. Anguelov and M. Angelova, Methodology for effectiveness in applying for grant funding for energy efficiency of enterprises, 2021 17th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2021, pp. 1–4, doi: 10.1109/ELMA52514.2021.9503051.
- [15] Goranova, S., & Anguelov, K. Critical review of Bulgarian legislation related to circular economy. *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, 2024, 1, 168–172. <https://doi.org/10.17770/etr2024vol1.7965>
- [16] P. Stoyanov and K. Anguelov, Corporate Social Responsibility Reporting: Information System Requirements, 2025 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1–5, doi: <https://doi.org/10.1109/COMSCI67172.2025.11225210>.
- [17] Zinoviev, V.; Koeva, D.; Tsankov, P.; Kutkarska, R. Review of Artificial Intelligence Applications in the Digital Energy and Renewable Energy Infrastructures. *Energies* 2026, 19, 1250. <https://doi.org/10.3390/en19051250>

Challenges in the Development of Autonomous Energy Microgrids in Bulgaria

Kiril Luchkov

Department of Economics, Industrial
Engineering and Management
Technical University of Sofia
Sofia, Bulgaria
kiril.luchkov@tu-sofia.bg

Mihail Chipriyanov

Department of Strategic Planning
Tsenov Academy of Economics
Svishtov, Bulgaria
m.chipriyanov@uni-svishtov.bg

Galina Chipriyanova

Department of Accounting
Tsenov Academy of Economics
Svishtov, Bulgaria
g.chipriyanova@uni-svishtov.bg

Abstract — The study analyzes the challenges facing the implementation of autonomous energy microgrids in urban areas in Bulgaria. In principle, their potential for achieving energy independence and decarbonization has been established. However, their implementation is hindered by factors such as a certain institutional vacuum linked to the lack of an appropriate legal framework, outdated distribution infrastructure, and social barriers in the management of condominiums. A model for an "energy cluster" is proposed. The aim of the study is to facilitate the transition to a horizontal ecosystem. Within this framework, energy is managed as a shared resource. The desired outcome corresponds to achieving a high degree of sustainability and economic stability at the local level.

Keywords — *microgrids, artificial intelligence, energy communities, sustainable development.*

I. INTRODUCTION

Globally, the market for decentralized energy systems is experiencing a real boom. Forecasts by the European Commission (EC) for the transition to Net-Zero predict that over 50% of European households will generate their own clean energy by 2030. This trend is driven by the widespread penetration of the sharing economy in the energy sector and the urgent need to relieve centralized networks. Therefore, the study of models such as „energy clusters“ is particularly important for countries in transition like Bulgaria. In our country, the lack of a flexible framework risks isolating the local market from European technological flows.

In contemporary energy theory, the transition to “smart neighborhoods” is emerging as a leading European practice for achieving energy independence [1]. Unfortunately, however, the implementation of autonomous energy microgrids in Bulgaria remains at a standstill due to a critical institutional vacuum and outdated infrastructure [2].

This study aims to analyze the obstacles to the design and implementation of these systems in the Bulgarian urban environment. At the same time, it seeks to propose a workable mechanism for overcoming them. To achieve this goal, three main tasks have been defined:

- identifying regulatory, technical, and organizational barriers;
- assessing the potential for adapting global experience in energy trading to the specificities of local condominium ownership;
- developing a model for an “energy cluster.”

The main thesis is that transforming residential neighborhoods into active “energy communities” is possible through the creation of specialized energy clusters. The process requires synergy between blockchain and AI technologies, combined with the introduction of „regulatory sandboxes“ in national legislation to allow for the testing of decentralized models in pilot zones.

The logic of the research process and the specific stages of the applied methodology are illustrated in Fig. 1.

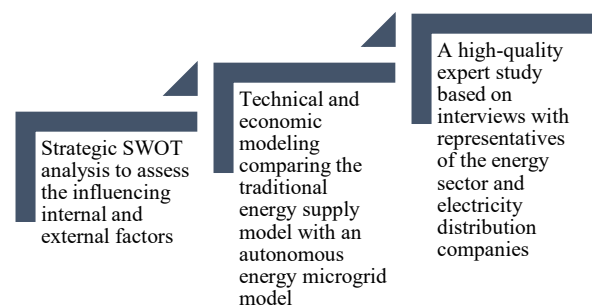


Fig. 1. Stages of the methodology used.

Source: Authors' own research.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.166>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

II. THEORETICAL FRAMEWORK AND GLOBAL EXPERIENCE

At the heart of autonomous microgrids lies the concept of peer-to-peer (P2P) energy trading [3]. It applies the principles of the sharing economy to the energy sector. The theoretical model of P2P platforms allows individual consumers to trade their surplus energy directly with one another [4]. This approach bypasses traditional centralized intermediaries [5]. It improves the management and utilization of locally generated renewable energy. At the same time, it creates economic incentives for investment in storage capacity. In the scientific literature, P2P trading in particular is viewed as a socio-technical innovation. Through it, market power is decentralized. This enables the formation of market-based pricing at the local level [6].

The experience gained in this field in developed Western countries provides an opportunity to study best practices. This is particularly true in countries such as the Netherlands and the Scandinavian region. In these countries, the high degree of applicability of so-called “smart neighborhoods” has been established. Projects in Amsterdam or energy communities in Denmark use blockchain for automated management of energy flows [7]. This takes place within closed communities. These case studies show that the integration of smart grids allows, in certain cases, for nearly 100% energy self-sufficiency for household needs. To ensure their success, modern digital technologies and the creation of a relevant regulatory environment are needed.

In the context of sustainable development, microgrids are a particularly important tool for increasing sustainability [8]. In general, centralized energy systems are highly susceptible to cascading failures or cyberattacks [9]. In contrast, autonomous grids can continue to power infrastructure in local mode [10]. In this way, they transform energy into a flexible and adaptive service capable of responding to external shocks.

The study seeks to answer the following research questions:

- **RQ1:** What are the critical regulatory and technical barriers preventing microgrid deployment in the Bulgarian context?
- **RQ2:** Is the proposed „Energy Cluster“ model economically viable compared to the centralized status quo?

III. MATERIALS AND METHODS

The scientific approach in this study is based on an analysis aimed at assessing the applicability of autonomous microgrids in the specific Bulgarian context. The methodological framework is structured in three main stages:

3.1. Strategic SWOT Analysis

A descriptive SWOT analysis is applied to assess the internal and external factors influencing the implementation of the „microgrid“ model. The method facilitates the identification of the advantages of decentralized production relative to institutional

weaknesses and external threats. We expect the analysis to serve as a basis for determining strategic priorities in the design of smart neighborhoods.

3.2. Technical-Economic Modeling

The comparative cost modeling method was used to assess effectiveness. A comparison was conducted between:

- Traditional model. Costs for centralized power supply, including the price of energy, grid services, etc.
- Autonomous model. Calculation of the energy cost, including initial capital investments for renewable energy sources (RES) and storage systems, operating costs, and potential savings from the absence of transmission fees.

The modeling aims to determine the point of economic efficiency for autonomous systems at current market levels in Bulgaria.

The comparative modeling is based on a standard residential block (entrance) with a total average monthly consumption of 8,500 kWh (average 420–450 kWh per household). A combined price (energy + distribution + taxes) of 0.24 BGN/kWh was applied for the traditional model. The levelized cost of energy (LCOE) was calculated in the autonomous model, considering a 30 kWp solar installation and a 15 kWh battery. Initial results show that the initial investment is significant [11]. In parallel, the operating costs per kWh in the Energy Cluster fall to approximately 0.11 - 0.14 BGN/kWh over a 15-year life cycle. This represents a potential long-term reduction in energy costs of nearly 45% compared to current market prices.

The calculation of LCOE is based on the following standard formula:

$$LCOE = \frac{\sum_{t=1}^n \frac{I_t + M_t}{(1+r)^t}}{\sum_{t=1}^n \frac{E_t}{(1+r)^t}}$$

where:

- I_t represents the initial investment,
- M_t are the annual maintenance and operational costs,
- E_t is the energy generated in year t , and r is the discount rate (assumed at 5% for this study).

3.3. Qualitative Expert Study

To validate the theoretical conclusions, a semi-structured expert interview was conducted with 9 representatives from the energy sector and the management of electricity distribution companies. The study aimed to identify the attitudes of network operators toward decentralization. The focus was on technical concerns regarding grid balancing and potential conflicts of interest during the transition to P2P trading [12]. The chosen approach provides an empirical basis for formulating management-oriented recommendations.

The empirical part of the study was carried out between January and March 2026. The selection of experts was purposeful, ensuring that participants had at least 5 years of professional experience in energy network management or regulatory issues. The interviews were conducted and

lasted an average of 45 minutes each. The data collection process was designed to establish the current market sentiment regarding the implementation of decentralized systems in the Bulgarian energy sector.

The panel of experts included:

- Senior Grid Engineers from major distribution system operators (DSOs) (3);
- Legal Experts specializing in Energy Law (2);
- IT Architects for Decentralized Systems (2);
- Representatives from Renewable Energy Associations (2).

IV. RESULTS

The study's findings identify three key groups of barriers that hinder the development of autonomous microgrids in Bulgaria [13]. These shortcomings create an environment characterized by high investment risk and low operational predictability.

To quantify the expert consensus, the identified barriers were rated on a scale from 1 (lowest impact) to 5 (highest impact). The results are summarized in Table 1.

TABLE 1. EXPERT ASSESSMENT OF BARRIERS TO AUTONOMOUS MICROGRIDS IN BULGARIA

Category of Barrier	Identified Key Issue	Mean Impact Score (1-5)	Consensus Level
Institutional	Lack of licensing regime for local operators	4.8	Very High
Technical	Predominance of one-way smart meters	4.2	High
Socio-organizational	Fragmentation of ownership in condominiums	4.5	High
Technical	Lack of real-time data exchange infrastructure	3.9	Moderate

Source: Authors' own research.

The data in Table 1 show that the institutional vacuum and the legal status of microgrids are perceived as the most significant obstacles. Experts emphasize that technical problems can be solved through investments. At the same time, the social and legal framework requires a fundamental change in national policy.

The study also includes an analysis of the technical readiness of existing urban distribution segments. The existing technical gaps require an estimated infrastructure investment of EUR 8,000-12,000 per residential building (entrance) to achieve full autonomous compatibility and integration of intelligent management systems. The main problem in the national legal framework is the complete absence of a licensing regime for "local energy operators." Current legislation (including the Energy Act) does not recognize the microgrid as an independent legal entity capable of managing local production and consumption. Potential energy communities are forced to operate within

the framework of outdated regulations designed for large centralized producers. The lack of a clear legal status blocks the possibility of legally sharing energy. It hinders the definition of pricing models for intra-community payments. All of the above makes microgrids practically illegal or economically unfeasible.

The technical analysis identifies a significant lag in the digitization of the transmission infrastructure. The effective operation of an autonomous microgrid requires the widespread deployment of smart metering devices [5]. These devices support two-way real-time metering. In Bulgaria, the majority of installed meters are designed for one-way consumption metering. This makes it impossible to precisely balance decentralized energy flows. The lack of a reliable infrastructure for data collection and exchange effectively means that smart load management and P2P trading remain technically unfeasible [14].

The socio-organizational barrier stems from the specifics of the Condominium Management Act. The process of making collective decisions on investments in shared energy assets (such as rooftop solar panels or shared batteries) is extremely difficult. This is due to high quorum requirements and the lack of effective mechanisms for enforcing shared obligations. Mistrust among owners, combined with cumbersome legal procedures for registering associations, limits opportunities for collective financing. In practice, energy democratization faces the challenge of fragmented ownership. Residential neighborhoods become a complex structure to manage, with low credit ratings and a high degree of internal conflict.

V. DISCUSSION

In response to the problem areas identified so far, we propose the creation of a so-called Energy Cluster. This is a specialized legal entity that brings together neighbors and property owners within a given neighborhood. The cluster functions as a new type of energy cooperative. It owns and manages shared assets (solar panels, batteries, charging stations). This model allows for the pooling of consumption, and the achievement of economies of scale in the purchase of equipment, as well as in maintenance. The cluster acts as an interface to the national grid. It improves the management of internal energy distribution, transforming the community into a flexible market participant.

To overcome mistrust and automate complex internal distribution processes, the model integrates blockchain and artificial intelligence (AI).

- Blockchain technology is used to create a decentralized ledger of transactions [16]. This enables fully transparent, automated, and instant energy settlements between neighbors in real time. No central accounting authority is required.
- AI algorithms take on the role of a „virtual dispatcher“. They forecast consumption patterns and generation capacity. They automatically determine when to charge the batteries, when to draw energy from the shared resource, and when to

sell the surplus to the external grid. This technological synergy eliminates the human factor from operational management and ensures maximum economic efficiency of the microgrid.

The integration of AI algorithms leads to the optimization of energy flows. Simulation data shows that predictive balancing of the „virtual dispatcher“ can increase the community’s self-consumption ratio (SCR) from 35% (unmanaged) to over 72% (AI-managed). By strategically discharging the batteries during the peak window from 18:00 to 21:00, the cluster can avoid the highest grid tariffs. As a result, an additional 18% annual savings in balancing costs can be achieved. This efficiency increase is crucial for the financial success of the cluster model in an environment of an unstable energy market.

To further illustrate the advantages of the proposed energy cluster, a comparative analysis was performed based on the techno-economic modeling described in the methodology. Table 2 presents the structural and economic differences between the current situation and the decentralized cluster approach.

TABLE 2. COMPARISON BETWEEN TRADITIONAL CENTRALIZED MODEL AND PROPOSED ENERGY CLUSTER MODEL

Feature	Traditional Model (Status Quo)	Proposed Energy Cluster (AI/Blockchain)
Energy Flow	Unidirectional (Grid to Consumer)	Bi-directional (P2P and Grid-interactive)
Price Control	Centrally regulated	Market-based local pricing
Grid Losses	High (due to long-distance transmission)	Minimal (localized balancing)
Decision Making	Individual/Fragmented	Collective/Automated via AI
Resilience	Susceptible to cascading failures	High (autonomous local operation)

Source: Authors’ own research.

The data in Table 2 show that the Energy Cluster replaces the energy source. And more importantly, it fundamentally changes the management logic. By using artificial intelligence as a “virtual dispatcher,” the community can reduce its dependence on the external grid by up to 40-60% during peak hours, depending on storage capacity. This transition shifts the focus from energy as a commodity to energy as a shared service.

Implementing this model requires the urgent introduction of so-called “regulatory sandboxes.” These are controlled environments in which the legislature allows temporary exemptions from general energy regulations for specific pilot neighborhoods. In these zones, energy clusters should be granted the right to operate microgrids without the licensing regime of large electricity distribution companies, to test P2P trading models, and to apply flexible pricing. We are convinced that the experience gained from these pilot projects will serve as a basis for scaling up the concept at the national level. Provisions of the Energy Act will be refined. Overall, this will transform Bulgaria into an active participant in the digital energy transformation.

VI. CONCLUSIONS

The analysis conducted demonstrates that autonomous microgrids are a mechanism with high potential for achieving the decarbonization of the urban environment [7]. They are the only sustainable solution for integrating the mass electrification of transportation and the transition to low-carbon heating. And they do so without overburdening the existing national infrastructure. By localizing the balance between production and consumption, microgrids minimize energy losses and transform urban neighborhoods into sustainable energy units capable of maintaining their functions even during major crises.

To overcome the identified barriers, a targeted change in the regulatory framework is needed, structured as follows:

- Reform of the Energy Act. Introduction of a legal definition for „energy community” and „microgrid“. This should be combined with simplified procedures for P2P trading and intra-community energy distribution.
- Update the Spatial Planning Act. Streamline procedures for installing renewable energy sources and storage systems in condominium buildings. In doing so, priority should be given to collective investment projects.
- Promotion of a National Program for the accelerated deployment of smart meters. The aim is to provide the necessary database for the operation of AI algorithms in microgrids.

The long-term vision outlined in this study envisions a transformation of the energy sector from a vertical monopoly to a horizontal ecosystem of shared services. In this model, energy ceases to be merely a commodity and becomes a socially shared resource managed through blockchain and AI technologies. Overall, the development of “smart energy communities” will strengthen the economic stability of households. Rational solutions will be implemented toward energy democratization.

VII. ACKNOWLEDGMENTS

This research was funded by the Bulgarian National Science Fund at the Ministry of Education and Science of Bulgaria under the Funding Competition for Fundamental Scientific Research Projects 2025, based on Administrative Contract № KP-06-N95/16 of 10 December 2025, for the implementation of Research Project № KP-06-PN95/45, SUNI № BG-175467353-2025-08-0248, titled „Epistemic robustness of artificial intelligence: A universal framework for evaluation in industrial and management systems“.

REFERENCES

- [1] Zinoviev, V. (2019). Challenges in the Power Supply for the Needs of Smart Cities, II International Conference on High Technology for Sustainable Development (HiTech), Sofia, Bulgaria, 2019, pp. 1-4, <https://doi.org/10.1109/HiTech48507.2019.9128268>.
- [2] Hartono, B. S., Budiyanto, Y., & Setiabudy, R. (2013). Review of microgrid technology. In International Conference on QiR (pp. 127–132). <https://doi.org/10.1109/QiR.2013.6632550>

- [3] Baroche, T., Pinson, P., Latimier, R. L. G., & Ahmed, H. B. (2019). Exogenous Cost Allocation in Peer-to-Peer Electricity Markets. *IEEE Transactions on Power Systems*, 34(4), 2553–2564. <https://doi.org/10.1109/TPWRS.2019.2896654>
- [4] Zhou, X., Guo, T., & Ma, Y. (2015). An overview on microgrid technology. In *2015 IEEE International Conference on Mechatronics and Automation (ICMA)* (pp. 76–81). <https://doi.org/10.1109/ICMA.2015.7237460>
- [5] Mengelkamp, E., Gärtner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Applied Energy*, 210, 870–880. <https://doi.org/10.1016/j.apenergy.2017.06.054>
- [6] Wang, H., & Huang, J. (2016). Incentivizing Energy Trading for Interconnected Microgrids. *IEEE Transactions on Smart Grid*, 9, 2647–2657. <https://doi.org/10.1109/TSG.2016.2614988>
- [7] Borkovcová, A., Černá, M., & Sokolová, M. (2022). Blockchain in the Energy Sector—Systematic Review. *Sustainability*, 14(22), 14793. <https://doi.org/10.3390/su142214793>
- [8] Hirsch, A., Parag, Y., & Guerrero, J. (2018). Microgrids: A review of technologies, key drivers, and outstanding issues. *Renewable and Sustainable Energy Reviews*, 90, 402–411. <https://doi.org/10.1016/j.rser.2018.03.040>
- [9] Bayindir, R., Hossain, E., Kabalci, E., & Perez, R. (2014). A Comprehensive Study on Microgrid Technology. *International Journal Of Renewable Energy Research*, 4(4), 1094–1107. <https://izlik.org/JA26PG88CE>
- [10] Eltamaly, A. M., & Ahmed, M. A. (2023). Performance Evaluation of Communication Infrastructure for Peer-to-Peer Energy Trading in Community Microgrids. *Energies*, 16(13), 5116. <https://doi.org/10.3390/en16135116>
- [11] Anguelov, K., Angelova, M. (2021). Methodology for effectiveness in applying for grant funding for energy efficiency of enterprises, 17th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2021, pp. 1–4, <https://doi.org/10.1109/ELMA52514.2021.9503051>.
- [12] Lin, H., Guo, Y., & Xu, Y. (2026). Impact of P2P Trading on the Operation of the Distribution System Operator. In *2026 IEEE PES International Meeting (PES IM)* (pp. 1–5). <https://doi.org/10.1109/PESIM67009.2026.11438640>
- [13] Keskinis, S., Elmasides, C., Kouveliotis-Lysikatos, I., Marhavalas, P. K., Hatziaargyriou, N. D., Stergiopoulos, F., Pompodakis, E., Fantidis, J. G., Makrides, G., & Delianidis, N. (2026). Integrating Safety into Microgrid Sizing: A Systematic Review. *Energies*, 19(9), 2098. <https://doi.org/10.3390/en19092098>
- [14] Petrova, D. An Alternative Approach to Reducing Aging of Innovative Industrial Products in Terms of Industry 4.0, Environment. Technology. Recourses – Proceeding of the 13-th International Scientific and Practical Conference, Rezekne Academy of Technologies, Rezekne, Latvia, 2021, ISSN1691-5402, Online ISSN 2256-070X, p. 274-280. <https://doi.org/10.17770/etr2021vol3.6507>
- [15] Baig, M.J.A.; Iqbal, M.T.; Jamil, M.; Khan, J. (2023). Blockchain-Based Peer-to-Peer Energy Trading System Using Open-Source Angular Framework and Hypertext Transfer Protocol. *Electronics*, 12, 287. <https://doi.org/10.3390/electronics12020287>
- [16] Stoyanov, P., Anguelov, K. (2025). Corporate Social Responsibility Reporting: Information System Requirements, 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5, <https://doi.org/10.1109/COMSCI67172.2025.11225210>.

An Integrated Approach to the Security of Energy Infrastructure: Problems and Innovative Solutions

Kiril Luchkov

Department of Economics, Industrial
Engineering and Management
Technical University of Sofia
Sofia, Bulgaria
kiril.luchkov@tu-sofia.bg

Mihail Chipriyanov

Department of Strategic Planning
Tsenov Academy of Economics
Svishtov, Bulgaria
m.chipriyanov@uni-svishtov.bg

Galina Chipriyanova

Department of Accounting
Tsenov Academy of Economics
Svishtov, Bulgaria
g.chipriyanova@uni-svishtov.bg

Abstract — The study analyzes the security of energy infrastructure. The need for an integrated approach that overcomes the limitations of traditional security models is argued. Methodologically, a combination of system analysis, qualitative risk assessment and scenario modeling is applied. Through this approach, structural vulnerabilities are identified and threats are classified. The study establishes that the effectiveness of modern technological solutions depends on their integration with organizational and management mechanisms. An integrated security management model is proposed, aimed at increasing the resilience of energy infrastructure.

Keywords — Artificial intelligence, Cyber-physical systems, Energy infrastructure, Resilience

I. INTRODUCTION

The security of energy infrastructure is being established as one of the central dimensions of modern national and international security [1]. Today, the energy sector is no longer an isolated industrial sphere and is becoming a complex, multi-layered socio-technical system [2]. Recent reviews further indicate that artificial intelligence is increasingly embedded in digital energy infrastructures through applications such as anomaly detection, predictive maintenance, forecasting and autonomous optimization [3]. Security is now a dynamic process requiring continuous adaptation.

Existing approaches and structures operate independently, without sufficient coordination in real time. Comparable studies in power-distribution mobile teams also demonstrate that algorithm-supported coordination can significantly improve response speed, resource deployment and operational effectiveness in critical network environments [4]. As a result, gaps in situational awareness are created that can be exploited in

complex attacks. This problem reflects a structural deficiency in current security architectures. Hence the need for an integrated approach.

The present study aims to analyze the main problems related to the security of energy infrastructure and to propose a model for overcoming them. The main thesis is that the protection of energy systems in the context of hybrid threats can be achieved by encompassing the dimensions of security in a single analytical framework.

II. THEORETICAL AND LITERATURE REVIEW

The concept of „energy security“ has traditionally been viewed as a function of the availability and access to energy resources. This approach has gradually proven to be insufficient. Cherp and Jewell propose a significant change. They define energy security as a state of low vulnerability of important energy systems [5]. This perspective allows the inclusion of new risks related to infrastructure interdependence and technological transformation. However, the proposed framework does not provide sufficient tools for the analysis of specific vulnerabilities.

A similar expansion of the analytical horizon is also observed in the research of Sovacool. He introduces an interdisciplinary approach. His analysis emphasizes that energy systems should be viewed as complex socio-technical structures. Technological solutions are related to the institutional and social context [6]. As a result, a gap is formed in the literature, in which the social dimensions are well developed and technological risks are partially investigated.

Panteli and Mancarella develop a model that considers resilience as the ability of energy systems to prepare for and recover from extreme events [7]. A flexible understanding of security is introduced. In this regard,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.170>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Humayed et al. emphasize that modern infrastructures function as cyber-physical systems [8].

Buldyrev et al. demonstrate that interdependent infrastructure systems are vulnerable to cascading failures [9]. This is especially true for energy infrastructure, which is closely linked to communication and information systems. Aven criticizes traditional probabilistic models of energy infrastructure [10]. Instead, he proposes a holistic approach.

Based on the identified problems, it is assumed that the security of energy infrastructure should be considered as a result of the interaction between technological, organizational and human factors. It is this logic that allows for the formulation of more effective protection models in conditions of increasing complexity and uncertainty.

III. MATERIALS AND METHODS

The present study is based on an integrated methodological approach. It combines systems analysis, qualitative risk assessment and scenario modeling. Related methodologies used in emergency-response teams further confirm the importance of coordinated decision systems under high uncertainty and time pressure [11]. The choice of this design is determined by the nature of the energy infrastructure, which functions as an interconnected socio-technical system. In such an environment, classical models prove to be insufficient. They do not take into account the interdependencies between physical and digital components. Therefore, a step-by-step analytical framework is applied. It allows a sequential transition from identifying vulnerabilities to formulating solutions. This approach ensures logical consistency and methodological clarity.

The proposed model is synthesized in Figure 1, which presents the logical structure of the study.

The figure illustrates the sequence of methodological stages, as well as the cyclical nature of the analysis, in which the results are used to update the initial model.

Stage 1: System Analysis of the Energy Infrastructure

The first stage of the methodology, presented in Figure 1, involves an analysis of the energy infrastructure. Here, it is viewed as a „system of systems“ including physical, digital and organizational components. The analysis covers the interaction between industrial control systems, supervisory control and data acquisition (SCADA) systems and physical energy assets. Particular attention is paid to important nodes and dependencies that can become points of failure. This approach identifies the structural vulnerabilities of the system. The result is an analytical map of the infrastructure, which serves as the basis for the following stages.

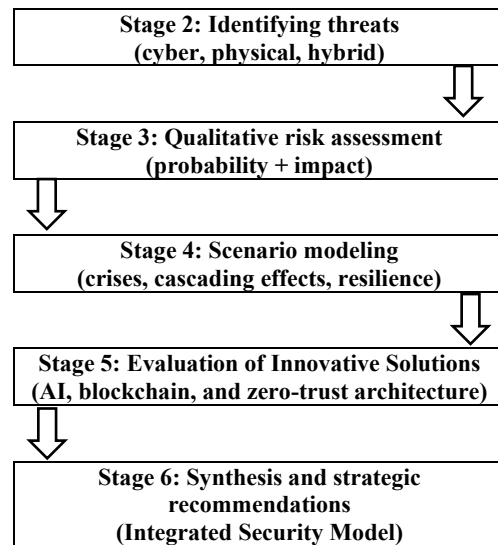
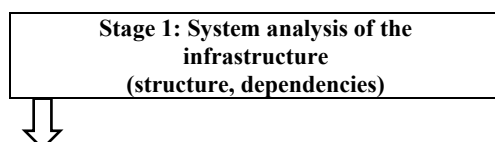


Fig. 1. Methodological model for analyzing the security of energy infrastructure

Source: Authors' own research.

Stage 2: Identification and Classification of Threats

The second stage builds on the system analysis by identifying threats. They are classified as cyber, physical and hybrid, in accordance with the logic presented in Figure 1. The analysis includes the development of typical impact scenarios. This allows for a transition from theoretical to applied analysis. As a result, a structured typology of threats is formed. This typology is decisive for the risk assessment.

Stage 3: Qualitative Risk Assessment

The third stage reformulates the identified threats into assessable risks. A qualitative approach is used, based on two criteria - probability and impact. Risks are classified into categories, which allows prioritization of protective measures. Particular attention is paid to events with low probability but high impact. This stage is a central part of the model. It connects the analysis with management decisions. The approach is consistent with the integrated logic of the methodology. The result is a clear picture of the risk profile.

Stage 4: Scenario Modeling and Resilience

The fourth stage involves the development of crisis scenarios and analysis of the system's resilience. The scenarios cover different types of attacks and failures, including hybrid impacts. The behavior of the system under different conditions is analyzed. Particular attention is paid to cascading effects. The results support the development of solutions.

Stage 5: Evaluation of Innovative Solutions

The fifth stage is aimed at evaluating modern technological solutions, such as artificial intelligence, blockchain and zero-trust architecture. Their ability to improve security is analyzed. Their applicability in a real environment is assessed. Of particular importance is their

integration with existing systems. This stage connects theory with practice. This stage represents the main contribution of the study.

Stage 6: Synthesis and Strategic Recommendations

The final stage summarizes the results and formulates strategic directions. The emphasis is on an integrated approach. The recommendations are aimed at increasing resilience. In this stage, the overall model is formed. It can be applied at different levels. This completes the methodological framework.

IV. RESULTS

The application of the methodological model (Figure 1) allows us to provide an analytical characterization of the structural properties of risk in the energy infrastructure. Already at the level of the system analysis, it is established that the vulnerability is not evenly distributed. The disruption of the functionality of digital management systems does not lead to local effects, but to the propagation of effects throughout the system. This means that the risk has a clearly expressed structural logic and cannot be considered as a random phenomenon. The analysis also shows that digitalization increases the density of these dependencies. Security management becomes increasingly complex. Thus, the first justified conclusion is formulated: the resilience of the system is a function of its internal structure, and not only of external protective mechanisms.

TABLE 1 RISK PRIORITIZATION BASED ON THE PROBABILITY-IMPACT RATIO

Threat	Rating
SCADA attack	Medium probability, high impact
Physical sabotage	Low probability, very high impact
Hybrid attack	Low probability, critical impact
Internal threat	Medium probability, medium impact
Legacy systems	High probability, medium impact

Source: Authors' own research.

The highest risk arises in scenarios where cyber attacks are transferred to the physical level. This is realized in the direction of industrial control systems and supervisory control and data acquisition (SCADA) systems. As a result, their vulnerability has a multiplier effect and increases the likelihood of failures. Additionally, it is established that hybrid threats do not necessarily require high technological complexity [12]. This highlights the need for more effective coordination of different types of impact. At the same time, it is observed that internal threats and legacy systems further enhance vulnerability by creating conditions for an initial breakthrough. The synthesized risk assessment is presented in Table 1.

The data summarized in Table 1 highlight a paradox in modern energy infrastructure security: the threats with the highest potential impact often have lower predictability. For example, "legacy systems" present a high probability

of exploitation due to outdated software and unpatched vulnerabilities. Yet their impact remains categorized as medium, as their failure modes are typically localized. "Hybrid attacks" and "physical sabotage" exhibit low probability combined with very high impact, capable of causing system outages. A shift to predictive and intelligence-driven security operations is required. This will favor the allocation of mitigation resources in proportion to the systemic severity of the risk, not just its frequency.

Risk assessment and scenario modeling reveal that the behavior of the system is characterized by the presence of cascading effects [14]. This creates serious difficulties in the early detection of threats. The analysis shows that this phase is the most important for risk management. As a result, it is confirmed that classical security indicators are not sufficient to assess the real state of the system. The results of the individual stages are summarized in Table 2.

TABLE 2 COMPARISON OF METHODOLOGICAL STAGES WITH THE OBTAINED ANALYTICAL RESULTS

Stage	Conclusion
System analysis	High interdependence
Identifying threats	Dominance of hybrid risks
Risk assessment	Prioritize high-impact events
Scenarios	Nonlinear propagation of effects
Technologies	Limited stand-alone effectiveness
Synthesis	An integrated model is needed

Source: Authors' own research.

Table 2 demonstrates that each step of the methodology leads to a qualitatively new level of understanding of risk. This allows us to formulate a third conclusion: security should be viewed as a dynamic process. Such an approach requires continuous adaptation of protection strategies. In this context, resilience becomes a key criterion for system effectiveness.

Blockchain technologies provide a high level of data integrity. More broadly, studies on reporting systems also confirm that data integrity and transparent information flows are central elements of effective governance architectures [13]. However, they cannot help in cases of physical vulnerabilities. Zero-trust architecture limits the spread of attacks, but requires a significant transformation of organizational processes. The summarized assessment is presented in Table 3.

TABLE 3 FUNCTIONAL ROLE OF INNOVATIVE TECHNOLOGIES IN SECURITY MANAGEMENT

Technology	Functional Role	Detection Efficiency	Implementation Complexity	Cost	Risk Level	Maturity
------------	-----------------	----------------------	---------------------------	------	------------	----------

AI	Anomaly detection	High	High	High	Medium	Medium
Blockchain	Data integrity	Medium	Medium	Medium	Low	High
Zero Trust Architecture	Restrict access	High	Very High	High	Medium	High
Algorithmic Coordination	Response support	High	Medium	Low	Low	High

Source: Authors' own research.

Multidimensional metrics (from Table 3) provide a comprehensive overview of operational and economic trade-offs. Innovative tools such as artificial intelligence and Zero Trust architecture offer high detection efficiency. At the same time, they require significant financial investments and present moderate organizational risks during implementation. Specialized solutions such as algorithmic coordination demonstrate a high level of technological maturity, which is combined with low risks during implementation. This makes them highly applicable to increasing network resilience. This assessment emphasizes that the selection of security technologies requires a balanced analysis of asset vulnerability, available budget and levels of systemic risk.

The effectiveness of technologies depends on their integration into the system. Their impact remains limited without coordination with organizational and management mechanisms. Solutions require integration. This sequence represents the main analytical contribution of the study. It allows the construction of a more precise security management model that takes into account the real complexity of the energy infrastructure. In this sense, the study offers a reasonable framework for its solution.

According to threat intelligence reports (such as IBM X-Force), the energy sector is among the top 3 most attacked industries. It accounts for 11% to 14% of all cyberattacks. Three macro trends support our model:

- OT Exploitation: Attacks against operational technologies (ICS/SCADA) are growing by over 25% annually, demonstrating the migration of threats to the physical layer.
- Ransomware and Extortion: Ransomware accounts for nearly 30% of incidents in the sector, escalating into hybrid extortion and physical sabotage threats.

- Geopolitical APT Aspects: Over 65% of sophisticated attacks are state-sponsored, relying on supply chain compromise and algorithmic manipulation.

With the expected 35% growth in smart grid devices over the next 5 years, traditional defenses are becoming obsolete. Modern risks require an architecture that combines zero-trust management, technical protection, and algorithmic team coordination.

V. DISCUSSION

The results obtained require a reassessment of the leading theoretical and practical approaches to the security of energy infrastructure. In the framework of this study, it was found that vulnerability is structurally concentrated. The results confirm the need to move to an integrated security model, in which the interactions between components are at the center of the analysis. Such an interpretation corresponds to the line in the studies of Cherp and Jewell. They emphasize vulnerability as the main criterion for energy security. The present study builds on this perspective because it concretizes it in cyber-physical systems. Thus, a higher degree of operationalization of the concept of „vulnerability“ is achieved.

The results show that the combined scenarios generate the highest level of risk. This observation questions the adequacy of existing classification models that distinguish threats by type without taking into account their mutual change. In this context, the vulnerabilities of industrial control systems (including SCADA systems) acquire leading importance. This confirms the thesis that the security of energy infrastructure should be considered as a cyber-physical phenomenon.

The present study supports the transition to a model based on resilience and continuous risk management. This means that security should be considered as a process.

VI. CONCLUSIONS

Based on the study, several specific scientific conclusions can be formulated that contribute to the development of the existing theoretical framework. First, the vulnerability of the energy infrastructure is structurally determined and concentrated in a limited number of points. Second, the leading risk arises from hybrid threats. Third, the behavior of the system in crises requires the use of scenario models for analysis. Fourth, the effectiveness of technologies depends on their integration into organizational and management processes. Fifth, resilience should be considered as a fundamental security criterion. Sixth, the lack of coordination between different levels of management is a significant factor for vulnerability.

One particularly defining area for future research is the specific analysis of high-risk AI systems in cyberattacks. This is the case when they are directed against critical energy infrastructures. Today, artificial intelligence (AI) is increasingly integrated into operational technologies. As a result, assessing the vulnerabilities of these high-risk algorithms against sophisticated cyberthreats will be

essential for maintaining system stability and preventing cascading network failures in the future.

At the strategic level, a move should be made to building comprehensive security management models [15]. This implies the development of policies that encourage coordination between different institutions and infrastructure operators. At the organizational level, mechanisms for real-time information exchange should be created.

VII. ACKNOWLEDGMENTS

This research was funded by the Bulgarian National Science Fund at the Ministry of Education and Science of Bulgaria under the Funding Competition for Fundamental Scientific Research Projects 2025, based on Administrative Contract № KP-06-N95/16 of 10 December 2025, for the implementation of Research Project № KP-06-PN95/45, SUNI № BG-175467353-2025-08-0248, titled „Epistemic robustness of artificial intelligence: A universal framework for evaluation in industrial and management systems“.

REFERENCES

- [1] Li, Q., & Song, Z., Research on Energy Security in the EU from a Trade Perspective: A Historical Analysis from 1991 to 2021. *Energies*, 18(14), 2025, 3801. <https://doi.org/10.3390/en18143801>
- [2] Papamichael, I., Voukkali, I., Vrionides, K., Loizia, P., Stylianou, M., Sospiro, P., Liscio, M. C., Naddeo, V., & Zorpas, A. A., An overview of critical energy infrastructure of the European Defence sector, *Energy Nexus*, Volume 19, 2025, 100483, ISSN 2772-4271, <https://doi.org/10.1016/j.nexus.2025.100483>.
- [3] Zinoviev, V., Koeva, D.; Tsankov, P., Kutkarska, R. Review of Artificial Intelligence Applications in the Digital Energy and Renewable Energy Infrastructures. *Energies* 2026, 19, 1250. <https://doi.org/10.3390/en19051250>
- [4] Angelova, M., Anguelov, K., Indicators for Evaluating the Effectiveness of Algorithmic Management in Mobile Teams of Power Distribution Companies, 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1-4, doi: [10.1109/ELMA65795.2025.11083518](https://doi.org/10.1109/ELMA65795.2025.11083518).
- [5] Cherp, A., & Jewell, J., The concept of energy security: Beyond the four As, *Energy Policy*, Volume 75, 2014, Pages 415-421, ISSN 0301-4215, <https://doi.org/10.1016/j.enpol.2014.09.005>.
- [6] Sovacool, B. K., Evaluating energy security in the Asia Pacific: Towards a more comprehensive approach. *Energy Policy*, 39(11), 2011, Pages 7472-7479. <https://doi.org/10.1016/j.enpol.2011.09.008>.
- [7] Panteli, M., & Mancarella, P., The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine*, 13(3), 2015, Pages 58-66. <https://doi.org/10.1109/MPE.2015.2397334>
- [8] Humayed, A., Lin, J., Li, F., & Luo, B., Cyber-physical systems security - A survey. *IEEE Internet of Things Journal*, 4(6), 2017, Pages 1802-1831. <https://doi.org/10.1109/JIOT.2017.2703172>
- [9] Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S., Catastrophic cascade of failures in interdependent networks. *Nature*, 464, 2010, Pages 1025-1028. <https://doi.org/10.1038/nature08932>
- [10] Aven, T., Risk assessment and risk management: Review of recent advances on their foundation, *European Journal of Operational Research*, Volume 253, Issue 1, 2016, Pages 1-13, ISSN 0377-2217, <https://doi.org/10.1016/j.ejor.2015.12.023>.
- [11] Angelova, M., Anguelov, K., Methodology for Evaluation Effectiveness and Efficiency of Algorithmic Management in Emergency Response Teams, 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1-5, doi: [10.1109/ELMA65795.2025.11083484](https://doi.org/10.1109/ELMA65795.2025.11083484).
- [12] Abraham, D., Houmb, S. H., & Erdodi, L., Cyber-Attacks on Energy Infrastructure - A Literature Overview and Perspectives on the Current Situation. *Applied Sciences*, 15(17), 9233, 2025. <https://doi.org/10.3390/app15179233>
- [13] Stoyanov, P., Anguelov, K., Corporate Social Responsibility Reporting: Information System Requirements, 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5, doi: [10.1109/COMSCI67172.2025.11225210](https://doi.org/10.1109/COMSCI67172.2025.11225210).
- [14] Wu, X., Zhao, S., Shen, Y., Madani, H., & Chen, Y., A Combined Multi-Level Perspective and Agent-Based Modeling in Low-Carbon Transition Analysis. *Energies*, 13(19), 2020, 5050. <https://doi.org/10.3390/en13195050>
- [15] D. Petrova. Intelligent, Innovative and Sustainable Industry in Bulgaria – prospects and challenges, Vide I. Tehnologija. Resursi - Environment, Technology, Resources, Proceeding of the 12th International Scientific and Practical Conference „Environment. Technology. Resources“, June 20-22, 2019, Rezekne, Latvia, Volume I, pp. 210-215, ISSN 1691-5402 – print, ISSN 2256-070X – online. <https://doi.org/10.17770/etr2019vol1.4188>

Fiscal Security and Non-Compliant Tax Conduct

Elina Marinova

Public Law Department

Angel Kanchev University of Ruse

Ruse, Bulgaria

elina_marinova@uni-ruse.bg

Abstract— Although the concept of national security has been extensively examined in scholarly literature, the notion of fiscal security has received limited academic attention. Fiscal security can be understood as a state of budgetary stability in which public financial interests are adequately safeguarded. Its core function is to ensure the availability of financial resources necessary for the stable and effective functioning of the state, and it represents a fundamental precondition for the effective implementation of public policies and the realization of governmental objectives. From this perspective, the level of fiscal security has effect directly over the level of national security, thereby requiring a thorough analysis of the concept.

Non-compliant tax conduct is a particularly serious threat to fiscal interests and has increasingly drawn the attention of the international community. Practices that circumvent and violate tax laws undermine the financial foundations of both the national security system and particularly in the European Union Member States. In addition to causing substantial losses to public budgets, such practices distort market competition, violate the interests of bona fide economic actors and the sustainable economic growth, and weaken public trust in the legitimacy of taxation and public governance in general. Developing a coherent theoretical framework for non-compliant tax conduct, including a clear distinction among various categories, as well as an analysis of their implications for national security, may improve legislative and law enforcement practices and strengthen inter-institutional cooperation.

Keywords— national security, fiscal security, non-compliant tax conduct, circumvention of tax law, violation of tax law

I. INTRODUCTION

Fiscal security plays a key role in national security, being both its important component and material base. It can be defined as such condition of the state budget where public financial interests are protected and safeguarded. Fiscal security ensures the stable and effective functioning of the state and is essential to the implementation of all state policies and objectives. In this regard it corresponds to all other types of security and serves as foundation for the national security system.

The consideration of fiscal security in the above context can also be derived, for example, from the framework outlined in the Updated National Security Strategy of the Republic of Bulgaria, adopted by the National Assembly on March 14, 2018. It identifies the implementation of effective policies by fiscal authorities, including the management of the revenue part of the state budget, as a national security priority, in cooperation with other state bodies and in partnership with private economic entities. It is explicitly stated that securing state budget revenues is essential for providing sufficient resources for all national security policies. The importance of economic and financial security is emphasized as sector policies which aim at maintaining macroeconomic and fiscal stability and building protective mechanisms to counteract the spillover effects of negative external developments.

The National Security Strategy of the Republic of Bulgaria (2018), similarly to the European Security Strategy “A Secure Europe in a Better World” of 12 December 2003, proposes a broad conception of national security that goes beyond the classical “force-based” understanding, linking it to the rule of law, democracy, and sustainable development. A number of contemporary scholars examine more non-traditional but also significant aspects of national security [1], [2], [3].

National security is widely studied in academic literature but fiscal security has received less attention [4], [5], [6]. At the same time, the link between fiscal security and national security is undeniable — state’s national security depends directly on the level of its fiscal security, and this is why an analysis of this concept is of particular importance. In this sense, the relevance of the issue of fiscal security is beyond doubt.

Non-compliant tax conduct is a particular threat to the state’s fiscal interests. The practices associated with it undermine the financial foundations of the national security system, as well as the security system of the states united in the European Union. In addition to significant losses to the public budget, they also lead to a distortion of market competition, harm to bona fide participants in

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.74>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

economic life, and economic growth, and undermine citizens' trust in the legitimacy of taxation and the fiscal system as a whole. In a criminological context, non-compliant tax conduct creates a favorable environment for the development of the shadow economy and organized crime, with a significant portion of the funds generated through such activities being used to finance other forms of criminal activity.

The lack of unified concept and standardized terms on non-compliant tax conduct comprise a significant problem in contemporary academic theory and legislative practice. This leads to difficulties and divergent interpretations in academic literature and legal practice. Therefore, theoretical research on non-compliant tax practices is both necessary and timely.

The present study is guided by the following research tasks:

- to develop a theoretical concept of fiscal security and to clarify its significance for national security;
- to examine the role of tax revenues in ensuring fiscal security;
- to define and systematically analyse the various forms of non-compliant tax conduct;
- to outline the practical contribution of the research, including the formulation of relevant proposals for improving Bulgarian legislation.

II. MATERIALS AND METHODS

The present study employs a multifaceted methodological approach, drawing on established research paradigms to elucidate the concept of fiscal security and the threats posed by non-compliant tax conduct. In this context, both special-legal and general scientific methods are applied. The integration of these approaches enables a comprehensive and systematic analysis, effectively bridging doctrinal interpretation with practical implications for legal regulation and enforcement.

A. Special-Legal Methods

These methods are of particular significance to the study, as they ensure a precise and coherent exposition of legal norms, definitions, and concepts relevant to the issues under examination:

- *The formal-dogmatic method* (legal dogmatics) investigates the legal norm "from within"—its text, structure, logical connections with other norms, interpretation, and application—to ascertain the exact content of applicable law. It systematically delineates corrective consequences for circumvention (e.g., denial of tax advantages) versus punitive sanctions for violations.
- *The comparative-legal method*, as a quintessential special legal technique, systematically juxtaposes legal norms, institutions, and practices across jurisdictions in order to identify optimal solutions and transnational alignments. In this context, the study conducts a comparative legal analysis of the applicable provisions in EU law and the legislation of the Member States, including Bulgaria, thereby highlighting similarities and differences

in anti-abuse mechanisms and in the regulation of various categories of unlawful conduct. On this basis, the conclusion puts forward proposals for improving Bulgarian legislation.

- *The interpretive (hermeneutic) method* deciphers legal texts through grammatical, logical, historical, and systematic approaches to discern the legislator's true intent. Applied here, it distinguishes the "spirit" from the "letter" of tax law in categorizing conduct: extra legem tax abuse, inter leges aggressive tax planning (exploiting loopholes); and contra legem offences.

B. Complementary Methods

- *The interdisciplinary method* integrates insights from cognate disciplines to enrich legal analysis beyond doctrinal confines. Here, it manifests through fusions of law with economics, political science, sociology and international relations theory. Economic perspectives underscore fiscal policy's role in macroeconomic stability and tax revenues' dominance. Political science links fiscal sovereignty to national interests. Sociological and historical lenses explore taxation's legitimacy and social contract preservation.
- *The systemic method* positions fiscal security within the broader architecture of national security, in line with multi-level categorizations and strategic frameworks.
- *Inductive and deductive reasoning* are employed to derive conceptual and definitional constructs from empirical data and to apply them within a normative legal framework.

III. RESULTS AND DISCUSSION

A. The Concept of Fiscal Security. The Collection of Tax Revenue as an Element of the Fiscal Security System.

"Security" is generally understood to mean the absence of risks and threats, or protection against them, thereby ensuring certainty and stability in the environment. The etymology of the term is linked to the Latin word *securus* ("secure"), which breaks down into two elements: *se* ("without") and *cura* ("care"). If we take the antonym "uncertainty" as our starting point, security can be viewed as a state of certainty in interactions. In a social sense, security as a state leads to trust, which in turn is the result of "the level of certainty in the mutual expectations of the actors" [7]. H. Morgenthau links security to national interests [8]. T. Koburov notes that, defined negatively, security means the absence of threats; defined positively, it upholds certain principles and values [9]. According to D. Yonchev, the term "security" denotes a state of equilibrium [10].

In one of the popular categorizations of security, it is divided into five main levels: individual security (personal, individual security), group security (security of a group of people), security of a single state, collective security (of several states or a union of states), and global security (universal, general) [11], [12]. In general, the first three are grouped under the category of "national security," while the remaining two fall under the category of "international security." N. Slatinski points out that "the growing interdependence in global, continental, regional,

and national processes blurs the boundaries between different levels of security. Issues inherent to the national security system are taking on aspects that were until recently characteristic of the international security system, and vice versa [13].

In light of the above ideas, we can define fiscal security as a state of equilibrium and order in the formation and use of public finances, in accordance with pre-established principles and values, whereby public financial interests are guaranteed and protected, as well as the financial and socio-economic foundations of the development of society and the state. Fiscal security is a key instrument for ensuring the stability and predictability of public administration as a whole, a prerequisite for the implementation of all national policies and objectives, and the foundation of the entire national security system.

The modern public finance system derives its legitimacy from the idea of providing mechanisms to manage uncertainty and ensure a predictable future and development within social systems. It serves as a code for legitimizing and protecting social groups and interests—through it interests, values, and goals are financially secured and prioritized as legitimate and urgent for implementation. The budget and public finances are not merely economic, financial, or legal matters, but also instruments for connecting and dividing, integrating and disintegrating communities and social groups that comprise them. M. Belov defines them as “phenomena of the system-sustaining culture of every society”. The author notes that the budgetary integration or disintegration of individuals, groups, classes, and institutions at national level is now heavily dependent on and linked to integration into the European and even global process of public finance management in the context of power inclusion and recognition within the European Union and the global political-financial community [14].

The concepts of finance, sovereignty, and security have always been closely intertwined in historical and political contexts. Finance is an important instrument of power within the framework of national sovereignty, but also beyond it, in the context of international relations. Sovereign states operate under structural constraints imposed by international financial mechanisms. Financial instruments are used to strengthen control over power and often serve the security and strategic interests of economically powerful states. According to M. de Goede, the spheres of finance and security are linked not only in an instrumental and causal sense (where finance is placed at the service of security or vice versa), but demonstrate a much deeper conceptual intertwining. Finance represents the economic counterpart of security [15].

Fiscal security can be additionally defined as a state of stable and predictable functioning of the public finance system in the state at the attributive level (order in public relations) and the institutional level (state bodies and mechanisms through which it is achieved). There are many factors on which fiscal security depends, but the leading role is played by an adequate fiscal policy that guarantees a balance between private and public interests, between

market-based and regulatory regimes in the financial system, an effectively functioning state administration, the lawful and effective implementation of the revenue and expenditure sides of public budgets, effective administrative and judicial oversight, and thereby the preservation of stability and confidence in the financial system. Ensuring stability and security for public finances, including the proper assessment and effective collection of taxes, is directly linked to the ultimate goals of the state’s fiscal policy—stability, security, and economic and social development. Stable and sustainable public finances, and consequently sustainable and inclusive growth in the Member States, are among the key priorities of the European Union.

Fiscal security corresponds to the exercise of a state’s fiscal sovereignty. Fiscal sovereignty reflects a state’s ability to conduct fiscal policy in accordance with its national interests, while taking into account international agreements and the state of the global political and economic environment. Fiscal sovereignty is at the core of state sovereignty in general, since material resources—in particular financial resources—are essential for the effective exercise of all functions related to sovereignty. In this sense, the treasury is the state itself. In a narrower legal-political context, fiscal sovereignty encompasses the state’s independent legal authority to establish, in the public interest within its territory, regulatory rules to govern and ensure the development of budgetary, tax, monetary, credit, foreign exchange, and customs legal relations.

Tax revenues are the main pillar of budget revenues both in Bulgaria and in the other member states of the European Union. Statistical data show that tax and social security revenues constitute the predominant share of state revenues. Data on the implementation of the Consolidated Fiscal Program (CFP) in Bulgaria as of December 2025 show that revenue from taxes and social security contributions accounts for 78.6% of total revenue under the CFP [16]. According to Eurostat data for 2024, the structure of general government revenue in the EU is as follows: For the European Union (EU) as a whole: Taxes account for 57.2% of total revenue, and net social contributions for 30.4% [17]. These figures clearly demonstrate the dominant role of tax and social security revenues in shaping public finances in Bulgaria and the European Union.

Tax revenues, as the main component of the state budget’s revenue side, are also the central source for financing public goods and services. Alongside fiscal considerations, taxation is often linked to additional socio-economic objectives—redistribution of national income to reduce social inequalities and maintain social cohesion, promotion of certain sectors of production, public healthcare and protection of the environment, and so on. There is hardly any phenomenon that exerts such a significant influence on a country’s economy and social sphere, and is at the same time so closely intertwined with culture and society, as taxes. From a historical and sociological perspective, the structure, method of

assessment, and collection of taxes in societies have always reflected their political philosophy, social organization, and societal development.

Taxes are an expression of the relationship between individuals and the government. The payment of taxes by citizens is a fundamental principle of a state-organized society. The fundamental importance of taxes for the construction of the state order and governance is reflected, for example, in the Bulgarian Constitution, which enshrines in Article 60 the obligation of citizens to pay taxes as a fundamental duty (same in Article 53 of the Constitution of Italy and Article 31 of the Constitution of Spain). In the modern state, taxes are established through universal legislative enactment, and their collection is ensured through the law enforcement activities of the executive and judicial authorities. Through legal enactment, the tax—which constitutes a financial constraint on individuals and an encroachment on private rights—is transformed into a lawful and legally binding payment [18]. At the same time, the laws guarantee the equality of citizens in taxation by establishing a general obligation unrelated to specific individuals. In this way, the law serves as a guarantee of the legitimacy of taxes in modern societies.

In order to fulfil their public purpose, both the law and taxes must, in all cases, be implemented according to pre-established rules rather than on an ad hoc basis, and there must be no discrepancy between the rules and their actual application. In this sense, effective tax collection is not only a prerequisite for the normal functioning of the public sector, the quality of public services, macroeconomic stability, curbing the shadow economy, and increasing transparency in economic life, but also a key mechanism for ensuring the principle of “equality before the law” and for maintaining the social legitimacy of the tax system.

B. Non-compliant tax conduct as a threat to the state's fiscal security. Concept and types

A key aspect of fiscal security is countering non-compliant tax conduct. This can have serious consequences for sound financial management and effective public financing in countries, thereby posing a threat to national security as well. Its most significant consequences are felt at the level of transnational business organizations whose activities span multiple national jurisdictions. Non-compliant tax practices affect both the efficiency and fairness of taxation. They deprive jurisdictions of significant revenue, thereby limiting tax systems' ability to serve redistributive purposes. At the same time, practices involving non-compliant tax conduct violate the principle of fair and proportionate sharing of the tax burden among individuals and undermine the legitimate interests of both states and regular taxpayers. As a result, fundamental principles of taxation such as neutrality, equality, and social acceptability are undermined. Such practices often generate and legitimize capital whose origin is linked to criminal activity. In order to formulate countermeasures, it is necessary to develop theoretical models that examine the nature and forms of non-compliant tax conduct.

We use the term “non-compliant tax conduct” as an umbrella concept encompassing various taxpayer's behaviour aimed at improperly avoiding tax obligations. Non-compliant tax conduct is carried out through **circumvention** or **violation of tax law**.

a) Circumvention of the Tax Law

Circumvention of the tax law refers to conduct through which a taxpayer seeks to obtain a tax advantage that contradicts the spirit (meaning and purpose) of the tax law, without the letter of the law directly opposing that tax advantage. Circumvention of tax law may consist of both an attempt to circumvent a tax-triggering factual scenario and an effort to comply with the letter of the law, but contrary to its purpose, by failing to meet the factual requirements for a tax relief or exemption. In such cases, there is often also an abuse of the otherwise permissible right to freely structure business activities for the purpose of tax savings [19], [20]. In this sense, the concepts of “circumvention of tax law” and “abuse of tax law” are closely related, as can be inferred from EU legislation and the ECJ's case law. The following can be considered subtypes of circumvention of the law: **abusive tax avoidance** and **aggressive tax avoidance**.

• Abusive tax avoidance

Abuse of tax law constitutes unlawful conduct whereby, through the use of fictitious legal forms, the link between taxation and the economic reality that underlies it is severed. Taxpayers give their actions and relationships a form (external appearance) that leads to tax exemption or the use of tax preferences without any real economic justification. This often involves “wholly artificial arrangements” which, although formally compliant with the law, are contrary to its spirit and purpose. (Case C-251/16 Halifax). To establish abuse, the ECJ requires the cumulative presence of two elements (the Halifax test): 1) objective—lack of economic reality and valid commercial reasons; and 2) subjective—the primary purpose of obtaining a tax advantage. This conduct may be characterized as “extra legem” [21]. As J. Ghosh argues, “the notion that “tax avoidance” is reprehensible constitutes an established legal norm of presumptive application in statutory interpretation” [22].

The prohibition on the abuse of tax rights is established in the General Anti-Abuse Rule (GAAR) in Article 6 of Directive (EU) 2016/1164 (ATAD 1) and in sectoral directives such as the Parent-Subsidiary Directive (2011/96/EU) – Article 11, the Merger Directive (2009/133/EC) – Article 15, and the Interest and Royalties Directive (2003/49/EC) – Article 5. It has been transposed differently in the legislation of the Member States. For example, a similar general clause is enshrined in § 42 of the German Tax Code (Abgabenordnung - AO), which states that tax law cannot be circumvented through the abuse of legal structuring options (Missbrauch von rechtlichen Gestaltungsmöglichkeiten). The approach in Bulgarian legislation is more case-specific, as the Corporate Income Tax Act (Art. 16) and the Tax and Social Security Procedure Code (Art. 19, Art. 57, para. 2, item 3, and Art. 122) provide specific examples and corresponding procedural rules related to tax abuse.

- Aggressive tax avoidance

This concept corresponds to the notion of “aggressive tax planning.” The theory states that it represents a transition between the rules—“inter leges”—established by several countries [23]. In principle, taxpayers’ behaviour remains within the bounds of the law (*intra legem*), but exploits technical features, loopholes, or inconsistencies in the legislation to achieve a tax advantage, which is generally undesirable under the tax legal order. According to H. Lenz, this behaviour is characterized by a focus on the literal interpretation (letter of the law) and little regard for the intent of the legislature (spirit of the law), with the behaviour “that aims to stop just before the illegal abuse of tax laws; the latter is called abusive tax avoidance (*extra legem*)” [21]. Unlike abuse, circumventing the law in this case does not necessarily require the creation of a “wholly artificial” structure.

Aggressive tax avoidance (aggressive tax planning) in the European and international legal sphere has been established as an undesirable tax practice, addressed legislatively, for example, through specific anti-abuse rules (SAARs)—such as rules limiting interest expenses, rules on controlled foreign companies, hybrid mismatches, exit tax under Directive (EU) 2016/1164 (ATAD 1) and Directive (EU) 2017/952 (ATAD 2), and through transparency measures such as those in Directive (EU) 2018/822 on mandatory automatic exchange of information on cross-border tax arrangements (DAC6), which sets out “typical features” of aggressive tax planning under Directive (EU) 2018/822 (DAC6), which are subject to disclosure to tax authorities.

The legal consequences provided for by the legislature in cases of circumvention of tax law are generally corrective in nature—the intended tax advantage is denied, and the tax liability is calculated as if the artificial arrangement had not taken place (Art. 6, para. 1 of Directive (EU) 2016/1164) or other corrective measures are taken—for example limiting interest expenses and exit tax when a company transfers assets, operations, or its tax residence outside the country, as a result of which the state loses its right to tax, etc. In some cases, as a corrective consequence of circumvention of tax law, legislation may provide for joint and several liability for tax due and unpaid by another person (e.g., Art. 177, para. 3, item 2 of the Bulgarian Value Added Tax Act). These measures essentially constitute a compensatory legal mechanism for the protection of the treasury and for addressing non-compliant tax conduct.

b) Violation of the Tax Law

This category covers explicitly unlawful acts that directly violate the letter of the law—constituting conduct *contra legem*. They can be broadly defined as tax offences—unlawful, culpable acts (actions or omissions) that are declared punishable by law. In the context of European Union law, international tax practice, and established English terminology, they are primarily associated with the concepts of tax fraud and tax evasion. Depending on the degree of public danger, tax offences are classified as either administrative violations or crimes.

- Administrative violation

Administrative violations are less serious form of tax offences—they constitute culpable acts that violate the established order of state governance in the tax sphere and are punished through administrative proceedings and by the tax authorities. They may be committed intentionally or negligently. In Bulgarian legislation, the general framework is regulated by the Administrative Violations and Penalties Act, while the specific offences are defined in the Tax and Social Security Procedure Code and in the substantive tax laws (VAT Act, Corporate Income Tax Act, Personal Income Tax Act, etc.). In the German Abgabenordnung, they are regulated in §§ 377–384. Instead, the tax administration in the United Kingdom imposes so-called civil penalties, primarily financial penalties for violations such as errors in returns (regulated under Schedule 24 of the Finance Act 2007) or failure to provide information.

- Tax crime

Tax crimes are the most serious tax offences, criminalized due to their significant public danger. They are regulated, for example, in Chapter Seven of the Bulgarian Penal Code, and §§ 369–376 of the German Abgabenordnung. Unlike administrative violations, crimes are committed only intentionally and are typically associated with tax evasion involving “large” or “particularly large” amounts (Art. 93, para. 14 of the Bulgarian Penal Code). Italy also applies a clear “double-track” model, distinguishing between administrative and criminal offences by introducing quantitative thresholds for evaded tax (Legislative Decree No. 74/2000). The aim is to avoid criminalizing less serious cases, which are effectively handled in administrative way.

In some cases, acts constituting circumvention of the law may constitute an offence; for example, the conversion of a company or transactions with related parties for the purpose of evading large amounts of tax constitute a crime under Article 255a of the Bulgarian Penal Code.

The legal consequences of all tax offences are punitive—they involve the imposition of administrative or criminal sanctions that affect the offender’s legal sphere by depriving them of benefits, restricting their rights, or imposing new obligations. They constitute a *sanctioning legal mechanism for the protection of the treasury*, serving as the most rigorous tool for countering and preventing non-compliant tax conduct.

IV. CONCLUSION

This study has rigorously conceptualized fiscal security as a state of equilibrium and order in the formation and utilization of public finances, aligned with pre-established principles and values, whereby public financial interests are guaranteed and protected, alongside the financial and socio-economic foundations of societal and state development. It serves as a pivotal instrument for ensuring the stability and predictability of public

administration, a prerequisite for all national policies and objectives, and the bedrock of the national security system.

The modern public finance system is legitimized by the idea of providing mechanisms to manage uncertainty and ensure a predictable future and development within social systems. Tax revenues, as the main component of the state budget's revenue side, are also a central source of funding for public goods and services. Geopolitical and financial-economic instability in the modern world reinforces the need for stable tax revenues, and in this context, the issue of non-compliant tax conduct is becoming increasingly relevant. Preventing and counteracting non-compliant tax practices plays a central role in building a just society and a strong economy, while simultaneously safeguarding the social contract and the rule of law.

The development of a unified theoretical concept of non-compliant tax conduct, distinguishing and outlining the legal consequences of the various categories of non-compliant tax conduct—as attempted in this study—contributes to both theory and practice, including improvements to the regulatory framework.

The practical applicability of these findings is multifaceted and targeted:

- For legislative activity, the analysis furnishes a theoretical scaffold for refining anti-abuse provisions, harmonizing with EU directives.
- Tax administration (e.g., National Revenue Agency) gains diagnostic tools for identifying hallmarks of aggressive planning and artificiality, enhancing audit efficiency and revenue recovery.
- Law enforcement agencies benefit from clarified delineations to streamline administrative-criminal delineations, reducing jurisdictional overlaps.
- The academic community acquires a unified conceptual framework, fostering interdisciplinary discourse on fiscal-national security nexuses.

In this regard, the following proposals for improving the legislation of the Republic of Bulgaria (*de lege ferenda*) may be advanced:

- Enactment of a general anti-abuse clause (GAAR) in Bulgarian tax law, mirroring ATAD 1 Article 6 and Germany's Abgabenordnung § 42, to supplant the current casuistic approach, capturing novel circumventions beyond enumerated cases.
- Legislative definition of "tax abuse" in the Tax and Social Security Procedure Code. Such a definition should mirror the established legislative model of the definitions for "administrative offense" under Article 6 of the Administrative Violations and Sanctions Act and "crime" under Article 9 (1) of the Penal Code. Adopting a general definition of tax abuse would yield profound practical benefits. It would enhance legal certainty for both taxpayers and tax authorities, foster a unified judicial interpretation, and improve the efficiency of tax audits by providing clear evidentiary criteria. Furthermore, it would ensure the full and correct transposition of EU law.

- Bolstering administrative-penal cooperation mechanisms to expedite hybrid cases. The existing Bulgarian framework, while providing a basis for cooperation, lacks the structured, mandatory protocols necessary to meet the ECJ's standards for coordination and efficiency. It is recommended that a formal, binding protocol for real-time information exchange between the National Revenue Agency and the Prosecutor's Office be developed, building on the legal basis of Article 26 of the National Revenue Agency Act. A shared digital registry should be established to track cases that have both administrative and potential criminal dimensions. For complex cases of suspected tax fraud, particularly those identified through mechanisms like DAC6, the formation of ad-hoc joint investigation teams comprising tax inspectors and prosecutors should be institutionalized.

In sum, fiscal security is indispensable to national security, with non-compliant tax conduct imperiling both amid geopolitical flux. This research reframes the issue strategically within EU-national security paradigms, advocating a robust, theoretically grounded arsenal for prevention and counteraction. Its conceptual innovations and reform proposals chart a path toward fortified public finances, equitable taxation, and resilient statehood.

REFERENCES

- [1] L. Lyubenov, Criminal Law Education as a Component of the National Security System of the Republic of Bulgaria, Environment Technology Resources – Proceedings of the 16th International Scientific and Practical Conference, 2025, pp. 155–161.
- [2] T. Markova, Economic Security in the Context of Industrial Security, in: Security and Defence, Iss.. 2, December 2023, National Military University Vasil Levski, pp. 137–147.
- [3] D. Sidova, D., Political Security as a Dimension of Freedom from Fear in the Context of Human Security, in: Security and Defence, Iss.. 2, December 2023, National Military University Vasil Levski, pp. 149–161.
- [4] A. Moldovan, Fiscal security of the state: conceptual basis for a new direction in ecosestate, in: Strategic Panorama (1-2), 2020, National Institute for Strategic Studies, Ukraine, pp. 86–96.
- [5] A. Kostyukov K. Maslov, The Role of National Fiscal Security and Tax Sovereignty in Collection of Taxes, in: Optimization of Organization and Legal Solutions concerning Public Revenues and Expenditures in Public Interest (Conference Proceedings), University of Białystok, Poland, 2018, pp. 449–460.
- [6] D. Criclivaia, I. Bruma, Fiscal Security: Identification of Threat Sources. In: Studia Universitatis Moldaviae. Exact and Economic Sciences Series: Mathematics. Informatics. Physics. Economics. Scientific journal, 2010, no. 7(37), pp. 116–120.
- [7] F.-X. Kaufmann, Sicherheit als soziologisches und sozialpolitisches Problem, in Soziologische Gegenwartsfragen, N.F. 31, Stuttgart, 1970, pp. 73–74.
- [8] C. Navari, Hans Morgenthau and the National Interest, Ethics & International Affairs, Vol. 30, Iss. 1, Spring, 2016, pp. 47–54.
- [9] T. Koburov, Situational Foreign Policy Analysis in the Field of Security, Sofia: King, 2009, p. 17.
- [10] D. Yonchev, In Search of Security, Sofia: East-West, 2014, p. 206.
- [11] N. Slatinski, Dimensions of Security, Sofia: Paradigma, 2000, pp. 44–46.
- [12] E. Manev, Global, Regional and National Security, Sofia: Softtrade, 2012, p. 225 et seq.
- [13] N. Slatinski, The Five Levels of Security, Sofia: Military Publishing House, 2010, p. 173.

- [14] M. Belov, *Financial Constitutionalism*, Sofia: Sibi, 2015, pp. 109–112.
- [15] M. de Goede, Financial security, in: *Finance and Society*, Vol. 3, Iss. 2, 2017, pp.161-165.
- [16] Ministry of Finance Bulletin on the Implementation of the State Budget and Key Indicators of the Consolidated Fiscal Program for December 2025.
- [17] Eurostat. *Government finance statistics*. [online] Statistics Explained , 2024, Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_finance_statistics [Accessed Apr. 6, 2026].
- [18] P. Stoyanov, *Tax Law*, Sofia: Bulgarian Academy of Sciences Press, 1994, p. 210.
- [19] R. Oberheide, Die Bekämpfung der Steuerumgehung, *Finanzwissenschaftliche Schriften*, Nr. 87, 1998, p. 30.
- [20] M. Lamensch.,M. Merkx, M. Schippers, I. van den Eijnde (Eds.), *Terra/Wattel European tax law.*, Volume II, Indirect taxation, Kluwer Law International, 2022, p.151.
- [21] H. Lenz, Aggressive Tax Avoidance by Managers of Multinational Companies as a Violation of Their Moral Duty to Obey the Law: A Kantian Rationale. *Journal of Business Ethics*, Volume 165, 2018, pp. 681–697.
- [22] J. Ghosh, *Key Ideas in Tax Law*, 5. The Reprehensibility of Tax Avoidance, Bloomsbury Academic, 2024, p.128.
- [23] P. Piantavigna, Tax Abuse and Aggressive Tax Planning in the BEPS Era: How EU Law and the OECD Are Establishing a Unifying Conceptual Framework in International Tax Law, despite Linguistic Discrepancies, *World Tax Journal*, February, 2017, p. 66.

A Comprehensive Approach to Assessing the Security of Built Heritage Sites Using Fire Risk Analysis and Evaluation Methodology

Galina Mileva

Department "Public Order and Security", Faculty of Law
Varna Free University "Chernorizets Hrabar"

Varna, Bulgaria

galina.mileva@vfu.bg,

ORCID [0000-0001-8035-5191](https://orcid.org/0000-0001-8035-5191)

Abstract — This article presents a comprehensive analysis of fire safety within monastic complexes in Bulgaria — designated as immovable cultural property — utilizing a field-tested risk assessment methodology. The study employs a multidisciplinary research design, integrating longitudinal data from over 500 buildings, with a focused statistical evaluation of 61 representative monastic sites. The methodological framework utilizes eight groups of risk indicators, categorized into unmanageable (variables), manageable (controllable), and neutral conditions. Descriptive and cluster analyses reveal a prevalent "Management-Driven Risk Profile", where the highest risk levels are concentrated in Technical Installations (Factor IV) and Legal/Organizational Measures (Factor VIII). A Pearson correlation analysis identifies a near-perfect association ($r = 0.99$) between administrative deficits and technical vulnerability, mathematically proving that fire risk is primarily systemic rather than environmental. To address these findings, the study substantiates a paradigm shift toward an "inclusive safety culture" and the strategic integration of municipal voluntary formations. The results provide an empirical foundation for a transition from reactive firefighting to a proactive, integrated risk management model for cultural heritage preservation.

Keywords — fire risk assessment methodology, immovable cultural property, inclusive safety culture, systemic vulnerability.

I. INTRODUCTION

The cultural heritage of Bulgaria is a vital component of its national wealth and a primary factor in the consolidation of Bulgarian cultural identity. This heritage is increasingly threatened by destruction, not only due to traditional causes of degradation but also as a result of

recent shifts in social and economic life, which have exacerbated destructive phenomena [1]. Consequently, the preservation of cultural property should not be viewed merely as physical conservation; instead, it must encompass a comprehensive set of strategic actions aligned with the contemporary requirements of society [2]. The protection of cultural heritage from fire has recently been redefined as a global priority, necessitating a holistic and proactive management approach [3].

The value of immovable cultural heritage sites is such that they are not subject to authentic restoration; therefore, preventing damage and loss from fire is an imperative goal. This circumstance places the primary weight of protection on prevention. From this perspective, a precise and timely updated fire risk assessment is an indispensable management tool [4]. It is no coincidence that such assessment is a vital element in the fire protection management systems for immovable cultural property across European Union countries, designed to minimize both the probability of fire and the severity of its consequences should one occur [5], [6].

The fire protection of immovable cultural heritage sites can be viewed as a functional system, in which the dynamics and the extent of goal achievement are a function of those elements most susceptible to management influence. In this context, these elements can be presented as a system of legal, organizational, technical, educational, and other measures [7]. Through their practical implementation, these measures aim to align the fire protection of these particularly valuable national sites with the best European practices.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.126>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Three core elements of the fire protection management system for immovable cultural property, as adopted in European Union countries, have been identified [8]. The most critical link in the mechanism for organizing the implementation and conduct of fire safety policy is the fire safety manager. The second pillar is the legally regulated and mandatory fire risk assessment [9]. The third essential element is the mandatory installation of a reliable fire detection and alarm system [10].

Various methods exist for developing specific risk assessments, one of which is the fire risk assessment. Since the primary objective of fire safety is to prevent and limit the impact of risk factors on protected sites — with human life and health being the highest priority — widely recognized fire risk assessment methods are extensively utilized in fire safety practice [11]. However, the specific nature of cultural heritage requires a paradigm shift in how these methods are applied.

The objective of this study is to diagnose the systemic fire risks within Bulgarian monastic heritage and to substantiate a transition from reactive firefighting to a proactive, risk-management-based preservation model. The applied approach facilitates an assessment of diverse factors, revealing the optimal interaction between variable, manageable, and neutral conditions. By identifying the optimal causality between these elements, the effectiveness of fire protection can be significantly enhanced.

II. MATERIALS AND METHODS

This research is based on a longitudinal study design, spanning nearly two decades of monitoring fire risk within Bulgarian monastic heritage. The data acquisition process was conducted in two primary phases: an initial large-scale empirical field study (2006–2007) involving 228 architectural sites, followed by a systematic expansion and update of the database to include over 500 individual buildings by 2025 [12]. For the purpose of the current statistical analysis, a representative sample of 61 active monastic complexes was selected to ensure a contemporary and rigorous evaluation of systemic risk factors [2].

This study employs a multidisciplinary approach, integrating field observations with a specialized fire risk assessment methodology tailored for historical structures. The analysis focuses on the data gathered from the selected 61 monastic complexes, all of which are designated as immovable cultural property. The methodological framework is based on the systematic evaluation of eight distinct groups of risk indicators, categorized into three functional domains: variables (unmanageable factors), controllable (manageable) parameters, and neutral conditions [7]. The selection and weighting of these risk indicators align with the latest international standards for classifying fire hazards in historic buildings, ensuring technical consistency with contemporary safety protocols [13]. Data acquisition was conducted through on-site surveys and structured audits aimed at evaluating technical installations, organizational preparedness, and the physical characteristics of the sites.

Statistical processing, including Pearson correlation and hierarchical cluster analysis, was performed to identify systemic dependencies between risk groups and to determine the optimal causality between variables within the fire protection management system.

III. RESULTS AND DISCUSSION

A. A New Approach to Fire Risk Assessment in Built Heritage

Due to the specific value and protected status of such sites, in addition to safeguarding human life and health, these buildings must be viewed not only through the strictly professional lens of the fire specialist but also from the perspective of the stakeholder — the owner, the tourist, and the ordinary citizen. Therefore, a new approach to fire risk assessment is required [5]. This approach should not only account for indicators such as the building's functional purpose, geometric dimensions, structural characteristics, fire load, type and number of technical systems, evacuation capabilities, presence and volume of combustible materials, occupancy, casualty rates, and emergency aid costs. Instead, it must also incorporate indicators regarding the value of the site itself, the presence of movable assets and property, internal and external security, the existence of internal fire safety regulations and their enforcement, and the competence and readiness of personnel to react adequately in the event of a fire or other emergency situations.

It is evident that there is no universal way to conduct a fire risk assessment for all immovable cultural heritage sites. Nevertheless, certain elements of this process must be standardized to develop a unified algorithm — that is, the assessment process needs to be formalized. This would allow for comparable results to be obtained regardless of differences in the input data, providing a basis for choosing between various risk treatment strategies, such as avoidance, transfer, mitigation, or reduction.

At first glance, an acceptable level of fire safety should be achieved through the precise and full application of fire safety and building codes. In practice, however, it appears that these codes have few points of convergence with risk assessment methods. In fact, the regulatory requirements used in risk assessments are most often transformed into various types of checklists. Thus, they become a static and limited tool for verifying whether a given building complies with fire-technical and construction requirements. While checklists allow for the rapid identification of problems, they do not determine the significance of the risks. Their significance must be calculated separately using complex statistical methods [9].

Risk analysis via checklists (checklist analysis) is an approximate, qualitative method. It is a versatile and flexible approach that is easily applied at any operational stage. This method can be considered a unified baseline for risk analysis and assessment, as its results provide the foundation for employing various other methodologies. Checklists comprise a set of indicators that reflect and identify different types of hazards, as well as the potential for undesirable events of various natures — such as

incidents, accidents, emergencies, or catastrophes. They are developed based on the actual, existing state of the site, as well as the processes and activities being conducted within it.

Checklists are structured to encompass potential, latent, and manifest hazards for all components of the site under investigation. They address both the general and specific aspects of the analyzed entity, depending on the level of detail applied to the hazard control indicators.

Specialized literature pays particular attention to calculating the impact of so-called “aggravating factors” and “mitigating factors”. The presence of these factors, through corresponding coefficients, serves to adjust the overall value of the risk indicator.

Since risk must be studied not only qualitatively but also quantitatively, a specific measurement procedure is applied. Measuring the various facets and properties of risk involves identifying and utilizing facts that can serve as their qualitative characteristics. These facts include a wide range of events, attributes of phenomena and processes, behavioral acts, assessments, and judgments. In practice, these specified facts function as risk indicators.

Indicators allow for the precise formulation of questions within the checklist, as well as the determination of the response structure. The selection of indicators is tailored to the nature of the site and the conditions under which the risk must be established.

B. Proposed Methodology

The proposed fire risk assessment checklist for immovable cultural heritage sites consists of eight groups of questions (indicators). Their responses are evaluated using coefficients that represent the varying relative weight of each risk factor, calculated via a specialized methodology. The indicators used for fire risk assessment in these sites can be classified into the following groups:

- I. Location and Value of the Site.
- II. Building Characteristics.
- III. Evacuation.
- IV. Technical Installations Description.
- V. Functional Use (Building Occupancy).
- VI. Visitor Profile and Occupancy Characteristics.
- VII. Arson Protection (Indicators).
- VIII. Legal and Organizational Fire Protection Measures.

C. Data Processing and Risk Matrix

The values (responses) of the indicators (questions) are arranged in a specific sequence to form a measurement scale. In hazard investigation and risk analysis, three primary types of measurement scales are utilized: nominal, ordinal, and interval scales. For enhanced clarity, the resulting severity assessments for the risk indicators from each group are compiled into a specifically designed table at the end of the checklist. Since the indicators across the

different groups in the fire risk assessment checklist for immovable cultural property carry varying relative weights relative to the overall fire risk value (ranging from 10% to 15%), a weighted average severity score must be calculated for the indicators in each group. These represent the most critical metrics of the study, as the highest values will serve as the basis for formulating conclusions and proposing specific measures to reduce the building's final risk rating. Based on the proposed risk matrix (Table 1), it is determined whether the fire risk for the immovable cultural heritage site is low, moderate, or high.

TABLE 1 RISK MATRIX AND QUANTITATIVE RANGES

Risk Level	Low Risk	Moderate Risk	High Risk
Score Range	0.10 – 0.36	0.37 – 0.63	0.64 – 0.90

D. Empirical Foundation and Field Research

The results of the first-of-its-kind broad-scale empirical field study, conducted between 2006 and 2007, examined 228 architectural sites — immovable cultural heritage — across twenty regions in Bulgaria regarding their fire safety [12]. These findings demonstrated a definitive need to continue the data collection process in order to monitor risk levels within these sites. This, in turn, prompted an even more detailed investigation and led to the development of the aforementioned methodology for fire risk analysis and assessment. By the end of 2025, it has been utilized to study more than 500 sites designated as immovable cultural property throughout the country.

The overarching conclusion drawn from the data so far points to a consistently high level of fire risk in Bulgarian monasteries [1]. These distinctive religious sites — perched on remote peaks or nestled within formidable mountain ranges — are widely distributed across Southeast Europe and the Near East, yet few have retained their original architectural integrity.

E. Scope and Representativeness

These findings are derived from a comprehensive study of over 60 monastic buildings and complexes in Bulgaria, which hold the status of immovable cultural property of world, national, and local significance. According to official data, there are 215 monasteries under the jurisdiction of the Bulgarian Orthodox Church, 122 of which are currently active. These sites represent a significant asset for the development of religious tourism in the region, attracting a constant flow of visitors which necessitates specialized safety measures [14].

F. Unmanageable Factors and Location Risk

Unmanageable indicators — such as site location, building type, building age, original functional use, and climatic and geographical conditions — are factors that may be favorable, obstructive, or neutral regarding fire protection. The first two categories are of particular importance for hazard and threat assessment, as well as for the organization of fire protection. One of the objective and immutable factors is their location — often in forested

areas, far beyond populated settlements, etc. This is an indicator with a negative impact on the level of fire protection, insofar as the current fire safety system, centered around the Chief Directorate “Fire Safety and Civil Protection” (CDFSCP) and private fire services, is concentrated in urban areas [15]. A reduction in this risk component could be achieved by implementing compensatory measures aimed at improving organization, technical equipment, and the emergency response preparedness of the permanent residents within the monastic complexes [16].

G. Historical Context and Conservation Challenges

All monastic buildings — designated as immovable cultural property — were constructed during the Middle Ages and the National Revival period. During these eras, the materials used and the architectural and engineering solutions differed significantly from today's regulatory requirements regarding structural integrity, fire resistance of construction materials, evacuation standards, etc. For an overwhelming majority (over 90%) of the studied sites, these historical discrepancies remain in effect. Furthermore, the scope of the risk increases significantly when considering the movable cultural assets housed within them — icons, church plate, wall paintings, frescoes, works of art, valuable ethnographic objects, period furniture, manuscripts, historical documents, photographs, and more.

H. Manageable Indicators and Targeted Impact

In the applied methodology for fire risk analysis and assessment, the values of the so-called “manageable indicators” provide particularly valuable information. These indicators represent characteristics and conditions upon which a targeted impact can be exerted to achieve changes that enhance the effectiveness of fire protection. These indicators can be classified into several groups: legal and regulatory, organizational, technical, educational, informational, and special (fire-technical and fire-tactical).

I. Evacuation and Emergency Preparedness

In over 72% of the investigated sites, the indicator values related to the capacity for rapid, adequate, and timely evacuation closely approach the upper threshold of the “moderate risk” range, with a clear trend toward “high risk” [6]. This is primarily due to the lack of theoretical and practical evacuation drills and control exercises. In cases where these are conducted incidentally, a formalistic approach is often adopted solely for the purpose of maintaining compliance documentation. Occupants lack clearly defined duties regarding their actions in the event of a fire or other hazards, possessing instead only a vague understanding of their expected behavior during emergencies. Furthermore, a significant majority of the sites lack emergency lighting, as well as adequate signage and designated evacuation routes.

J. Internal Regulatory Framework and Management Control

Survey data indicate that in a vast majority of the investigated sites, internal regulatory frameworks are either non-existent or not known to be in effect. Thorough

knowledge of documentation requirements by staff, continuous updates by management, and the maintenance of active communication with fire departments and emergency services can significantly enhance preparedness and ensure adequate responses to adverse events. The absence of an internal regulatory framework diminishes the capacity for effective fire safety control and severely limits — or in some cases, precludes — the possibility of fire safety management.

Special attention should be drawn to the problem related to the capacity of the people working both in the administrative as well as in the professional spheres of preservation activities. There is also a lack of well-trained decision-makers at the local level, not to mention private owners (or local representatives of the Holy Synod of the Bulgarian Orthodox Church) who have cursory legal knowledge and almost no such in terms of modern approaches for the protection of their own cultural valuables, based on risk assessment and risk management. It turns out that none of the survey respondents know and therefore does not apply risk assessment as a preventive approach to managing the risks in their property.

K. Technical Equipment and Conservation - Sensitive Fire Suppression

The type of technical equipment, and specifically the fire suppression system within a historical building, is of paramount importance. A critical consideration in this context is the potential for secondary damage — irreversible harm caused not by the flames themselves, but by the fire suppression agents used during intervention [11]. Assets such as wall paintings, manuscripts, paintings, icons, and archives can be damaged or destroyed as much by fire as by the water, foam, or powder used in firefighting efforts. In Bulgaria, modern fire suppression technologies based on aerodynamic principles and the creation of water mist (aerosol curtains) remain relatively unknown and are consequently rarely implemented. These, along with gas-based suppression systems (e.g. Hypoxic Air System), are designed primarily to protect specific sites, such as buildings designated as immovable cultural property. Furthermore, it should not be overlooked that only a negligible number of the studied sites have implemented adequate organizational and technical access control measures against malicious acts by third parties — such as vandalism, hooliganism, theft, or graffiti [10]. In more than 83% of the investigated monastic buildings and complexes, the weighted average score for the severity of indicators within the fourth group “Technical Installations Description” is either at the upper limit of the “moderate risk” range or falls directly within the “high risk” category.

L. Methodological Analysis and Descriptive Statistics of Risk Factors

The initial stage in the quantitative assessment of fire safety within monastic complexes involves the application of descriptive statistics to evaluate the distribution and variability of the eight identified risk factor groups. This approach facilitates the identification of central tendencies within the dataset and highlights areas with the highest concentration of risk. By calculating the mean, median, and

standard deviation for all 61 surveyed sites, a baseline risk profile for Bulgarian monastic heritage is established. This statistical overview is instrumental in distinguishing between systemic risks — common to all sites — and specific outliers, while providing the necessary empirical foundation for subsequent cluster and correlation analyses. The following table (Table 2) summarizes the statistical parameters, emphasizing the critical impact of technical infrastructure and organizational preparedness on overall fire vulnerability. The individual distribution of these scores is visually represented in Fig. 1, highlighting a significant heterogeneity among the surveyed sites [13]. While the majority of the monasteries fall within the moderate-to-high risk range (0.50–0.65), several sites approach the high-risk limit, and one specific outlier exceeds the critical threshold of 0.80. This visual evidence confirms that while fire risk is a widespread challenge, certain locations suffer from acute systemic protection failures that require immediate, prioritized intervention.

TABLE 2 DESCRIPTIVE STATISTICS OF FIRE RISK FACTORS (N=61)

Factor Group	Mean	Median	Std. Deviation (SD)	Min Value	Max Value
I. Location & Value of the Site	0.421	0.441	0.054	0.256	0.510
II. Building Characteristics	0.505	0.529	0.065	0.308	0.612
III. Evacuation	0.505	0.529	0.065	0.308	0.612
IV. Technical Installations	0.631	0.662	0.081	0.385	0.766
V. Functional Use (Occupancy)	0.463	0.485	0.059	0.282	0.561
VI. Visitor Profile	0.505	0.529	0.065	0.308	0.612
VII. Arson Protection	0.547	0.574	0.070	0.333	0.663
VIII. Legal & Organizational Fire Protection Measures	0.631	0.662	0.083	0.385	0.766
Final Risk Assessment Score	0.526	0.552	0.068	0.320	0.638

Descriptive analysis shows that factors IV (Technical Installations) and VIII (Legal and Organizational Fire Protection Measures) present the highest risk levels across the 61 surveyed sites, both peaking at 0.766. The low standard deviation in Factor I (0.054) suggests that location-based risks are relatively uniform, whereas the management-driven risks (Factor VIII) vary significantly, highlighting a lack of standardized fire safety protocols in Bulgarian monastic heritage.

Analysis of Results:

Critical Risk Indicators (Highest Impact): Factors IV (Technical Installations) and VIII (Legal and

Organizational Measures) exhibit the highest mean values (0.631). This indicates that on a national scale, the systemic fire risk for Bulgarian monasteries is not primarily driven by their geographic location or intrinsic value, but rather by their technical condition and administrative preparedness.

Data Variability and Heterogeneity (Standard Deviation): Factor VIII shows the highest standard deviation (0.083), highlighting a significant “regulatory gap” between different sites. This suggests a lack of standardized fire safety protocols, where some monasteries are well-regulated while others remain critically neglected.

Distribution Symmetry: The proximity between the mean and median values across all categories suggests a normal distribution of the data. This enhances the statistical reliability of the findings, indicating that the sample is representative of the general state of monastic heritage in Bulgaria.

In conclusion, the quantitative analysis of the 61 monastic sites identifies a “Management - Driven Risk Profile”. While inherent factors such as location and architectural complexity contribute to the baseline hazard, the primary drivers of fire risk are anthropogenic and controllable. The perfect correlation between the high scores in Technical Installations and Legal Measures (Max = 0.766) underscores a critical need for policy intervention. Improving the legal and organizational framework is the most effective pathway to mitigating technical vulnerabilities and ensuring the long-term preservation of these cultural monuments.

M. Cluster Analysis of Fire Risk Profiles

Building upon the baseline descriptive statistics, a cluster analysis was conducted to categorize the 61 monastic sites based on the convergence of their risk profiles across the eight factor groups. The primary objective of this classification is to move beyond individual site assessment and identify shared patterns of vulnerability. Cluster analysis will allow us to see not only which monasteries are at risk, but also why – i.e. what are the common “weak points” of the different groups of sites. Since there are 61 sites in the full data set, clustering by each of the 8 groups of factors reveals specific patterns. A detailed cluster analysis by risk factor groups (N=61) follows in the section:

1. Location and Value of the Site (Factor I)

- “National Heritage” Cluster: This group includes the Rila Monastery, Bachkovo Monastery, and the Rock-hewn Churches of Ivanovo. These sites are characterized by exceptional historical and cultural value but face significant hazards due to remote or difficult geographic accessibility for fire-fighting equipment.
- “Local Significance” Cluster: Comprised of smaller monasteries (e.g., Balsha, Shiyakovtsi) with lower risk indices in this category, primarily due to better proximity to urban centers and simpler site layouts.

2. Building Characteristics and Architectural Vulnerability (Factor II)

- “Organic Materials” Cluster: Monasteries featuring predominant timber-frame constructions and historical wooden ceilings (e.g., Chiprovtsi, Divotino). Here, the risk of rapid fire spread is at its peak due to the high fuel load of the building materials.
- “Solid Structures” Cluster: Includes rock-hewn churches and more recent stone masonry constructions. While structural fire load is lower, these sites often present challenges in terms of ventilation and heat entrapment.

3. Evacuation Efficiency (Factor III):

- “Critical Access” Cluster: Sites with narrow entrances, steep staircases. These architectural constraints significantly hinder rapid evacuation.
- “Enhanced Safety” Cluster: Sites like the Kardzhali Monastery, where modern planning and restoration have integrated efficient evacuation routes.

4. Technical Installations (Factor IV)

- “High Technological Risk” Cluster: This is the most problematic group, led by Chiprovtsi (0.766) and Klisura (0.715) monasteries. Statistical data indicates a critical degree of wear in electrical grids and a lack of automated fire detection systems.
- “Maintained Systems” Cluster: Although the Rila Monastery shows a relatively high score (0.673), it remains lower than smaller sites, suggesting more consistent maintenance and professional technical oversight.

5. Functional Use and Occupancy (Factor V)

- “Mixed-Use” Cluster: Monasteries that integrate kitchens, residential quarters, and museum spaces. The risk of fire ignition from domestic activities is significantly higher here.
- “Liturgical/Monumental” Cluster: Sites like the Rock-hewn Churches of Ivanovo, which have minimal domestic activity but are vulnerable to risks associated with visitor negligence or candle usage.

6. Visitor Profile and Crowd Characteristics (Factor VI)

- “Mass Tourism” Cluster: Rila and Bachkovo Monasteries. The fire risk is directly linked to high visitor density, reflecting the broader trends in Bulgarian religious tourism where sacred sites function as major cultural and pilgrimage hubs [14].

- “Pilgrimage/Quiet” Cluster: Smaller monasteries with fewer but more frequent visitors, allowing for better site control and lower human-induced hazard levels.

7. Arson Protection and Negligence (Factor VII)

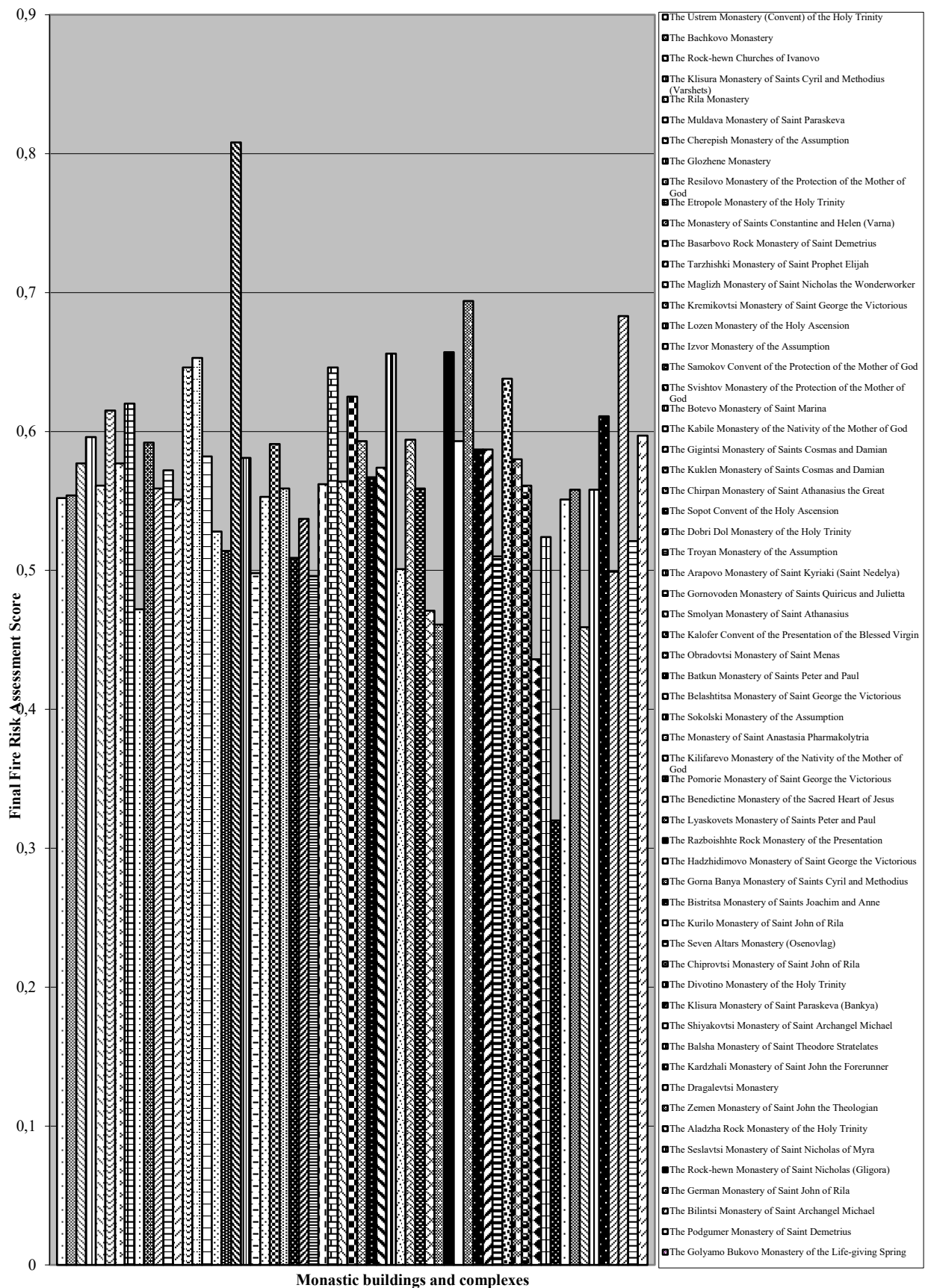
- “Unsecured” Cluster: Sites lacking 24/7 security or video surveillance systems.
- “Secured” Cluster: Sites with high levels of access control and monitoring, showing a strong correlation with Factor VIII (Legal Measures).

8. Legal and Organizational Measures (Factor VIII):

- “Administrative Deficit” Cluster: Sites with high final risk scores consistently show a lack of updated fire safety plans and staff training. This group confirms that technical vulnerability is often a symptom of administrative inaction.
- In summary, the group-specific cluster analysis demonstrates that Bulgarian monastic heritage is subject to a “dual-threat” model. While one group of risks is inherent (Location and Architecture), the most severe risks are anthropogenic (Technical Installations and Legal Measures). The fact that Factor IV and Factor VIII scores are consistently identical across the highest-risk clusters suggests that the modernization of technical infrastructure is impossible without a prior or concurrent reform of the legal and organizational fire protection framework.
- By employing a hierarchical clustering approach (Table 3), the study distinguishes between inherent structural risks — defined by architecture and geography — and manageable risks — defined by technical and administrative oversight [8]. This categorization provides a strategic framework for resource allocation, allowing for targeted fire safety interventions based on the specific risk typology of each group.

Discussion of Cluster Typologies:

- The “Management-Technical” Nexus (Cluster A): The most alarming finding is the emergence of Cluster A, where technical decay is directly correlated with administrative stagnation. For these 15 sites, fire risk is not an environmental inevitability but a result of prolonged systemic neglect. The convergence of high scores in technical installations and legal non-compliance creates a “perfect storm” for fire ignition and rapid spread.



7771

<https://doi.org/10.5552/3542026.vol1.126>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Fig. 1. Distribution of Final Fire Risk Assessment Scores across the 61 surveyed monastic buildings and complexes in Bulgaria.

TABLE 3 CATEGORIZATION OF MONASTIC SITES BY RISK CLUSTER (N=61)

Cluster Designation	Defining Characteristics	Representative Sites (Sample from N=61)	Aggregate Risk Intensity
Cluster A: Critical Administrative and Technical Failure	Maximum scores in Factors IV (Technical) and VIII (Legal). Characterized by obsolete electrical infrastructure and lack of emergency protocols.	Chiprovtsi, Klisura (Varshets), Divotino, and 12 other local sites.	High (0.58 – 0.64)
Cluster B: High Structural and Logistical Vulnerability	High scores in Factors I (Location) and II (Building Characteristics). Complex masonry or timber frames in remote geographic areas.	Rila Monastery, Bachkovo, Rock-hewn Churches of Ivanovo, and 8 mountainous sites.	Moderate-High (0.55 – 0.58)
Cluster C: Moderate Baseline Risk	Near-median scores across all factors. Represents sites with functional but aging protection systems.	Ustrem (Holy Trinity), Balsha, and 24 medium-sized monasteries.	Moderate (0.50 – 0.55)
Cluster D: Optimized Fire Safety Profile	Lowest scores across all indicators. Characterized by modern renovations, accessible locations, and updated legal documentation.	Kardzhali (St. John the Forerunner), Shiyakovtsi, and 10 recently restored sites.	Low (0.32 – 0.44)

Inherent vs. Controllable Vulnerabilities (Cluster B vs. Cluster D): The analysis distinguishes between sites like the Rila Monastery (Cluster B), where risk is dictated by its monumental scale and timber-heavy architecture, and sites like Kardzhali (Cluster D). While the former requires specialized suppression systems due to its "intrinsic" risk, the latter demonstrates how modern integration of safety standards can effectively mitigate the fire hazard index even in historic contexts.

In conclusion, the clustering of 61 Bulgarian monasteries reveals that fire vulnerability is predominantly a function of human intervention rather than environmental factors. The high concentration of sites within the "Critical Administrative Risk" cluster (Cluster A) underscores a significant deficit in the national strategy for heritage protection. To reduce the overall fire risk, policy focus must shift from general oversight to the specific remediation of technical and legal indicators. Transitioning

sites from Cluster A to Cluster C or D is achievable through standardized electrical modernization and the rigorous implementation of organizational fire safety mandates, independent of the site's geographic or architectural constraints.

N. Correlation Analysis of Fire Risk Factors

To determine the strength and direction of the relationships between the different risk indicators, a Pearson correlation analysis was performed across the dataset of 61 monastic sites (Table 4). The values in the Table 4 represent the Pearson Correlation Coefficient (r). In the context of cultural heritage fire safety, correlation analysis serves as a critical diagnostic tool, revealing how vulnerabilities in one sector (e.g., legal oversight) may amplify risks in another (e.g., technical infrastructure). By quantifying the degree of association between these variables, the study aims to identify the primary "risk drivers" — factors that have the most significant impact on the final risk assessment score. This statistical approach shifts the focus from isolated incidents to systemic dependencies, providing an empirical basis for integrated risk management. The analysis identifies Factors IV and VIII as the primary risk drivers.

TABLE 4 CORRELATION MATRIX OF RISK FACTORS (N=61)

Risk Factors	Location and Value of the Site	Technical Installations	Legal and Organizational Measures	Final Risk Assessment Score
I. Location and Value of the Site	1.00	0.95*	0.94*	0.98*
IV. Technical Installations	0.95*	1.00	0.99*	0.99*
VIII. Legal and Organizational Measures	0.94*	0.99*	1.00	0.99*
Final Risk Assessment Score	0.98*	0.99*	0.99*	1.00

*Correlation is significant at the 0.01 level (2-tailed).

Interpretation of the Correlation Data:

The Dominance of Anthropogenic Factors: The analysis reveals an exceptionally strong positive correlation ($r = 0.99$) between Factor IV (Technical Installations) and Factor VIII (Legal and Organizational Measures). This near-perfect correlation suggests that the technical safety of the monasteries is almost entirely dependent on the existence and enforcement of a legal and administrative framework. Statistical evidence confirms that where administrative documentation and fire safety protocols are absent, technical systems are invariably substandard.

Predictors of the Final Risk Score: Factors IV and VIII show the highest correlation with the Final Risk Assessment Score ($r = 0.99$), identifying them as the most influential predictors of overall fire vulnerability. In

contrast, while Factor I (Location and Value) remains significant ($r = 0.98$), it has a slightly lower impact on the final variance compared to the management-driven factors. This proves that human-controlled variables are more decisive for the safety of the sites than their geographic or historical characteristics.

In conclusion, the correlation analysis provides conclusive mathematical evidence that the fire risk in Bulgarian monastic heritage is systemic and management-dependent. The extremely high coefficients between technical, legal, and organizational factors indicate that these elements do not function in isolation but form a consolidated risk block. For policymakers and conservationists, these findings imply that technical upgrades (such as electrical modernization) will be ineffective without a concurrent strengthening of the legal and organizational fire protection mandates. Therefore, an integrated approach — addressing both the “software” (legal measures) and “hardware” (technical systems) of fire safety — is the only statistically viable path to reducing the final risk score of these cultural monuments. Furthermore, the integration of digital registers and GIS-based mapping represents a strategic advancement in monitoring the vulnerability of immovable cultural property in Bulgaria [17].

O. The Comprehensive Approach and Inclusive Safety Culture

Aligned with contemporary European safety frameworks, this study advocates for a paradigm shift toward an “inclusive safety culture” — a concept that has become central to modern security policies. This approach moves beyond traditional methods by promoting the active involvement of the entire monastic community, emphasizing that fire safety is not the sole responsibility of professional services, but a collective commitment. Establishing a functional synergy within this culture requires a clear understanding of the unique civil law status of the Bulgarian Orthodox Church and its monastic institutions [18]. In the Bulgarian context, this model should be expanded to integrate municipal voluntary formations, which are formally regulated by national law [16]. These units, together with the local community, represent a vital strategic resource capable of countering the geographic isolation of heritage sites and ensuring a more resilient and rapid defense system through all phases of protection: prevention, response, and mitigation [15].

IV. CONCLUSIONS

The findings of this study demonstrate that the fire vulnerability of Bulgarian monastic heritage is a multifaceted phenomenon, where technical decay is fundamentally a symptom of administrative stagnation. The objective of this research — to diagnose the current risk landscape and substantiate the need for priority interventions — has been achieved through the identification of a critical “Technical - Legal Nexus”. The empirical evidence confirms that standalone technical upgrades (e.g., electrical modernization) are statistically ineffective without a concurrent strengthening of the legal and organizational fire protection framework [7], [13].

To ensure the long-term preservation of these sanctuaries, three strategic goals must be prioritized:

- **Administrative Reform:** Achieving a functional synergy between state institutions and the Bulgarian Orthodox Church to implement standardized, mandatory fire safety protocols and updated internal regulations. This requires a precise alignment with the specific legal status of the ecclesiastical institutions [18].
- **Implementation of a National Risk Registry:** As a concrete policy measure, the study proposes the creation of a “National Registry of Fire Vulnerability for Cultural Property”. This centralized digital database would allow for real-time monitoring of the risk status of each monument, facilitating data-driven resource allocation and prioritizing emergency interventions based on the quantitative risk indices established in this methodology [17].
- **Community-Based Resilience:** Shifting toward an “inclusive safety culture” that leverages local residents and voluntary formations to overcome the logistical challenges posed by geographic isolation [16], [3].

In conclusion, the fire safety of Bulgarian monasteries is not an inevitable consequence of their age or location, but a manageable variable. Establishing a national risk-based monitoring system is the only viable path to protecting these guardians of national identity and ensuring they are bequeathed in their authentic form to future generations.

ACKNOWLEDGMENTS

The author expresses gratitude to the representatives of the Bulgarian Orthodox Church and the local fire services for their cooperation during the field surveys.

REFERENCES

- [1] G. Mileva, “Obstacles and Opportunities for Raising Cultural Heritage Disaster Prevention Awareness at the National Level in Bulgaria,” *Fundamental and Applied Researches in Practice of Leading Scientific Schools*, vol. 33, no. 3, pp. 18–24, June 2019. [Online]. Available: <http://farplss.org>. [Accessed November 30, 2019], <https://doi.org/10.33531/farplss.2019.3.05>.
- [2] Y. Stoyanova-Toneva, “Cultural-historical and educational resources of rural areas,” *Scientific Papers Series “Management, Economic Engineering in Agriculture and Rural Development”*, vol. 21, Issue 2, pp. 629–636, 2021. [Online]. Available: https://managementjournal.usamv.ro/pdf/vol.21_2/volume_21_2_2_021.pdf. [Accessed May 10, 2026].
- [3] UNESCO, *Fire Risk Management Guide: Protecting Cultural and Natural Heritage from Fire*. Paris, France: UNESCO Publishing, Nov. 2024. [Online]. Available: <https://www.unesco.org/en/articles/unesco-launches-guide-prevent-fires-cultural-and-natural-heritage-sites>
- [4] D. Soto, Y. Sánchez Suárez, A. Cabrera Hernández, and A. Hernández Nariño, “Heritage properties management in historic centers: subprocesses and main components,” *RSAN*, vol. 1, no. 62, pp. 85–92, June 2025. Available: Web of Science, <https://www.webofscience.com/>. [Accessed March 25, 2026], <https://doi.org/10.36097/rsan.v1i62.3489>.

- [5] E. Garcia-Castillo, I. Paya-Zaforteza, and A. Hospitaler, "Fire in heritage and historic buildings, a major challenge for the 21st century," *Developments in the Built Environment*, Vol. 13, 2023, 100102, ISSN 2666-1659. Available: ScienceDirect, <https://www.sciencedirect.com/science/article/pii/S2666165922000369>. [Accessed May 8, 2026], <https://doi.org/10.1016/j.dibe.2022.100102>.
- [6] S. Kincaid, "Fire prevention in historic buildings – approaches for safe practice," *The Historic Environment: Policy & Practice*, Vol. 13, Issue 3, pp. 361–380, 2022. [Online]. Available: Taylor&Francis, <https://www.tandfonline.com/doi/full/10.1080/17567505.2022.2098633#abstract>. [Accessed May 12, 2026], <https://doi.org/10.1080/17567505.2022.2098633>.
- [7] G. Mileva, *Izsledvane na sigurnostta na nedvizhimoto kulturno nasledstvo* [Research on the Security of Immovable Cultural Heritage]. Varna: Varna Free University "Chernorizets Hrabar", 2012, pp. 104–121, 308–323.
- [8] P. Vandeveldel *et al.*, *Fire Risk Evaluation to European Cultural Heritage: FIRE-TECH Decision Supporting Procedure, Users Guide*, 5th FP, Ghent University, Belgium, 2005, p. 19.
- [9] G. Mileva, "Otsenkata na riska kato osnoven element ot sistemata za upravlenie na požarnata zashtita na sgradi – nedvizhimi kulturni tsennosti" [Risk Assessment as a Core Element of the Fire Protection Management System for Buildings – Immovable Cultural Property], in *Proc. 6th Sci. Conf. with Int. Participation "Civil Safety 2011"*, Part II, Academy of the Ministry of Interior, Sofia, 2011, pp. 144–148.
- [10] Y. Guan, Z. Fang, and T. Wang, "Fire Risk Assessment and Daily Maintenance Management of Cultural Relic Buildings Based on ZigBee Technology," *Procedia Engineering*, Volume 211, 2018, p. 192–198, ISSN 1877-7058. Available: ScienceDirect, <https://www.sciencedirect.com/science/article/pii/S1877705817362276>. [Accessed March 20, 2026], <https://doi.org/10.1016/j.proeng.2017.12.004>.
- [11] L. Salazar, E. Paupério, O. Tikhonova, R. Figueiredo, and X. Romão, "A new fire damage index to assess the vulnerability of immovable cultural heritage," *International Journal of Disaster Risk Reduction*, Vol. 111, 2024, 104731, ISSN 2212-4209. Available: ScienceDirect, <https://www.sciencedirect.com/science/article/pii/S221242092400493X>. [Accessed May 8, 2026], <https://doi.org/10.1016/j.ijdr.2024.104731>.
- [12] G. Mileva, *Zashtita ot požari na nedvizhimite pametnitsi na kulturata* [Fire Protection of Immovable Cultural Monuments]. Varna: Varna Free University "Chernorizets Hrabar", 2009, pp. 49–53, 113–114, 151–156, 166–168.
- [13] A. Jurecki, W. Grześkowiak and M. Wieruszewski, "Current Standards for the Purposes of Assessing and Classifying Fire Hazards in Historic Buildings," *Fire*, vol. 8, no. 11, Art. no. 410, Jan. 2025. [Online]. Available: <https://www.mdpi.com/2571-6255/8/11/410>. [Accessed May 14, 2026], <https://doi.org/10.3390/fire8110410>.
- [14] A. Samer and M. Firkova, "Religious tourism of Bulgaria and Syria," *Scientific Works*, vol. 64, Issue 2, pp. 163–169, 2022. Available: <https://nauchnitrudove.au-plovdiv.bg/17-2-2022/>, [Accessed Aug. 8, 2025].
- [15] *Zakon za zashtita pri bedstviya* [Disaster Protection Act]. Promulgated State Gazette (SG) No. 102/19.12.2006, last amended and supplemented SG No. 60/07.07.2020. [Online]. Available: <https://www.lex.bg/laws/ldoc/2135540282>. [Accessed Apr. 26, 2026].
- [16] *Naredba za reda za sazdavane i organizirane na deynostta na dobrovolnite formirovaniya za predotvratyavane ili ovladyavane na bedstviya, požari i izvunredni situatsii i otstranyavane na posleditsite ot tyah* [Ordinance on the procedure for the creation and organization of the activities of voluntary formations for the prevention or management of disasters, fires and emergencies and the elimination of their consequences]. Promulgated State Gazette (SG) No. 50/03.07.2012, last amended SG No. 7/20.01.2026. [Online]. Available: <https://www.lex.bg/laws/ldoc/2135800522>. [Accessed Apr. 26, 2026].
- [17] Project Buzludza Foundation, "Digital Registers and Maps for Cultural Heritage Protection," in *Proc. Open Forum "Digitalization and Innovation for Cultural Heritage"*, Sofia, Bulgaria, Apr. 2026. [Online]. Available: <https://buzludza-project.com/forum/>
- [18] M. Kyoseva, *Civil Law Status of the Bulgarian Orthodox Church* (in Bulgarian). Sofia, Bulgaria: Zograf Monastery Heritage Foundation, 2024.

Reduction of the Specific Activity of Radioactively Contaminated Soil Using the High-Pressure Hydro-Cleaning Method

Musaev Maruffjan Nabiyeovich
Head of the Department "Life Safety"
(Ph.D., Professor)
Tashkent State Technical University,
Uzbekistan, Tashkent
promecology@mail.ru

Azizjon Azimjonovich Boboev
Department of "Automation and Control"
(PhD dotsent),
Navoi State Mining and Technological University
Uzbekistan, Navoi
azizjon.boboev@bk.ru

Feruza Azimjonova Boboeva
Department of "Social and Humanitarian Sciences" Navoi University of Innovations '
(PhD) Uzbekistan, Navoi
boboyevaf17@gmail.com

Tolibjonov Shoxjaxon Otabeko'gli
Department of "Automation and Control"
(student), Navoi State Mining and Technological University Uzbekistan,
Navoi
tolibjonovshoxjaxon97@gmail.com

Abstract — Radionuclides are mainly bound within soil layers and exist in the Earth's crust as mineral-like substances that are resistant to heat and electrical воздействия and can split into thin layers, making them difficult to wash out easily. Therefore, in order to extract radionuclides from radiation-contaminated soil layers and reduce their specific activity, it is necessary to separate them using various processing methods. Currently, conventional methods developed for treating radiation-contaminated soils include extraction using acids, alkalis, or other chemical reagents. These treatment methods require large amounts of chemical reagents, making them economically inefficient and difficult to apply to large volumes of contaminated soil.

Keywords — radioactive soil, radionuclides, soil decontamination, high-pressure hydro-cleaning, specific activity reduction, radiation contamination, soil remediation, hydro-mechanical treatment, environmental safety, gamma spectrometry.

I. INTRODUCTION

Radioactively contaminated soils represent a significant environmental and industrial safety challenge in modern conditions. This issue is particularly critical in mining and industrial areas, where radionuclides accumulate within soil layers and pose serious risks to both

the environment and human health. Radionuclides are typically strongly bound to fine soil fractions, making their removal by conventional washing methods difficult.

Traditional treatment methods, including extraction using acids and alkalis, are widely used; however, they require large amounts of chemical reagents and are economically inefficient. Moreover, these methods present environmental and technological limitations when applied to large volumes of contaminated soil.

Therefore, the development of efficient, cost-effective, and environmentally safe technologies for reducing the specific activity of contaminated soils is of great importance. This study investigates the application of a high-pressure hydro-cleaning method combined with soil dispersion and fractionation processes to separate radionuclides and reduce their concentration. The proposed technology minimizes the use of chemical reagents and improves the efficiency of soil remediation.

II. MATERIALS AND METHODS

To conduct the research, when studying the spatial and depth distribution, a regular sampling grid is established in

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.194>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

radionuclide-contaminated soil areas at intervals of 25–30 meters in the horizontal direction (along the X and Y axes). Samples are collected both at the contamination center and within a radius of 5–30 meters. This approach allows for a detailed assessment of variations in activity levels.

The distribution of activity with depth is determined by sequential sampling of soil layers at 15 cm intervals down to a depth of 0.8 meters. Experimental results indicate that radionuclide activity significantly decreases with increasing depth. Monitoring is carried out at four key time points: before treatment, immediately after treatment, and after 6 months and 1 year. This method makes it possible to evaluate both the immediate effectiveness of the technology and the long-term dynamics of changes in the radiation background [1-7].

High-resolution gamma spectrometers are used to quantitatively determine the concentrations of radium, potassium, and thorium. In addition, the granulometric composition and organic matter content, which influence radionuclide binding, are also analyzed [15-20].

In this study, a new technology aimed at reducing the volume of contaminated soil was applied by using a high-pressure washing method for the treatment of soils contaminated with radioactive elements. The implemented technology reduces processing costs by 15–20% compared to previously used high-temperature treatment (sublimation) methods and chemical extraction technologies [21-24].

In this technology, a dispersant is added to the contaminated soil, after which it is continuously disintegrated using a high-pressure flow of 4 MPa or higher. As a result, minerals that have adsorbed radioactive elements are separated from the aggregated soil and recovered, thereby partially neutralizing and reducing the volume of contaminated soil. The dispersant reduces the zeta potential of the aggregated soil, ensuring stable dispersion of fine soil particles and facilitating the separation process [8-12].

This process consists of the following main stages:

The first stage involves soil preparation, in which contaminated soil is mixed with water and dispersants and then fed into the soil supply unit. At this stage, solid particles in the soil are thoroughly mixed and prepared for subsequent technological processing. Uniform distribution of soil particles and effective mixing with dispersants improve the efficiency of the washing process [25,26].

The prepared mixture is delivered to the washing ejector using a high-pressure pump. The pump pressure is at least 4 MPa, which enables high-pressure washing of the soil and physical separation of particles. Through high-pressure washing, the ejector separates fine soil particles (<100 μm), thereby ensuring a reduction in contamination through physical means [27,28].

At this stage, layered and fine soil fractions are separated and directed to the sedimentation process for particle settling, where special reagents are added. These reagents promote the aggregation and settling of fine and

layered particles, which plays a crucial role in reducing radioactive contamination. This process also serves to optimize the particle size distribution within the resulting sediment [29, 30].

The settled soil is then passed through a dewatering unit, where excess water is removed. As a result, the processed soil is divided into particle size fractions: washed soil (20–100 μm) and layered soil (<20 μm). In the final stage, the dewatered soil is discharged via a vibrating screw conveyor and prepared for further processing or disposal [12-15].

As a result of this technological process, the level of soil contamination is significantly reduced, fine and layered particles are effectively separated, and radiation safety is ensured through sedimentation with reagents. Furthermore, the resulting soil is dried and stabilized, which reduces radiation and chemical exposure risks for workers and allows for environmentally safe and sustainable reuse.

III. RESULTS AND DISCUSSION

Figure 1 illustrates the process of separating hazardous radioactive substances through the dispersion and fractionation of soil composition. At this stage, soil aggregates are broken down into fine particles, allowing fractions bound with radioactive substances to become free. Subsequently, high-pressure washing and fractionation processes are carried out, resulting in the separation of coarse soil particles and fine fractions containing radioactive materials.

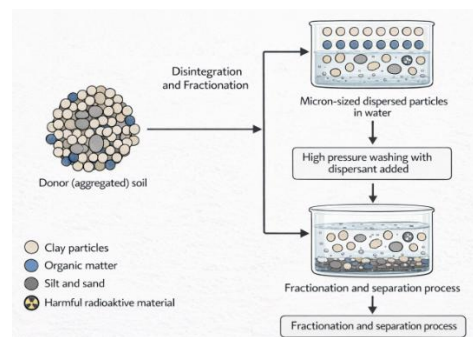


Fig. 1. Method for separating hazardous radioactive substances through dispersion and fractionation of soil composition.

The structure of the ejector used as a soil washing device is shown in Figure 2.

This device draws soil into a pipe with a diameter of approximately 50 mm and washes it using turbulent flows generated by a high-pressure stream. The addition of a dispersant under highly turbulent conditions produces an effective disintegration effect.

In this system, the contaminated soil, disintegrated by high-pressure washing, undergoes subsequent classification and separation processes, during which minerals that have adsorbed radioactive elements are selectively separated. The soil is then divided into washed soil and concentrated fractions, followed by dewatering.

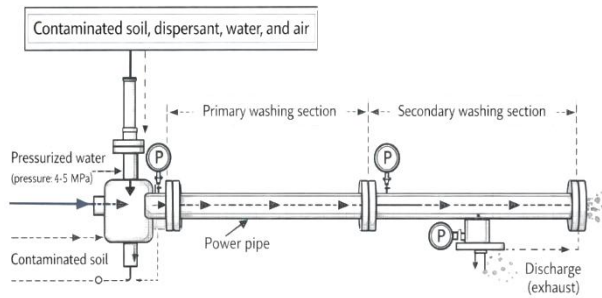


Fig. 2. Method for separating hazardous radioactive substances through dispersion and fractionation of soil composition.

The system shown in Figure 1 utilizes a vibrating screen, a screw conveyor, and a wet cyclone as classification devices.



Fig. 3. Photograph of a high-pressure cleaner (ejector).

For the experimental studies, soil samples were primarily collected from uranium geological exploration and extraction sites. Contaminated soils with radionuclide concentrations ranging from 7,500 to 41,700 Bq/kg were selected.

After the washing process, an increase in particle dispersion and partial surface cleaning is observed. In the case of enriched soil, the separation of fine fractions and the accumulation of active components in certain portions become evident.

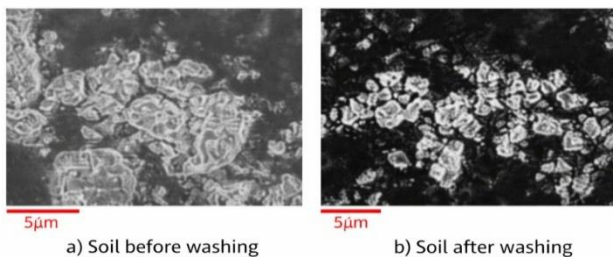


Fig. 4. SEM (Scanning Electron Microscopy) image of soil washed under high pressure.

The obtained results demonstrate the effectiveness of soil washing and enrichment technology and confirm that

it meets occupational safety and sanitary requirements in the remediation of radiation-contaminated areas.

Figure 5 shows the recovery rate of soil particles. The developed system demonstrated a recovery efficiency of 47–75% for soil particles with a size of less than 20 µm and 74–91% for particles with a size of 20 µm and larger.

These results indicate the effectiveness of the developed system in soil disintegration, particle classification, and recovery processes.

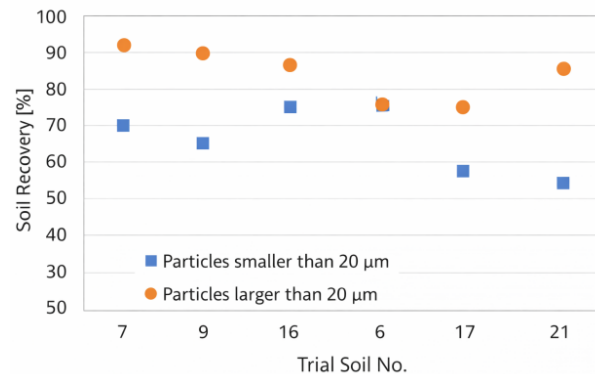


Figure 5. Recovery rate of soil particles

IV. CONCLUSION

The results of the conducted studies showed that the radiation condition of soil in workplaces of mining industry enterprises represents a significant risk factor for workers' health. During the study, it was determined that the specific activity of radioactive substances in soil initially varied within the range of 7,500–41,700 Bq/kg, with an average value of 15,800 Bq/kg. These values are considered high for industrial conditions and affect both external gamma radiation exposure and internal exposure through soil.

As a result of applying the proposed technology based on high-pressure washing and fractional separation, the concentration of radioactive substances in the soil decreased to 2,200–5,200 Bq/kg, with an average specific activity of 3,800 Bq/kg. This corresponds to an average reduction of about 76% compared to the initial condition, significantly lowering the radiation hazard level of the soil.

The reduction in soil activity was also reflected in the radiation doses received by workers. Before treatment, the annual external gamma radiation dose ranged from 0.8 to 1.8 mSv/year, while after treatment it decreased to 0.5–1.1 mSv/year, representing a reduction of approximately 1.4–1.7 times. Similarly, the internal radiation dose due to dust inhalation decreased from 0.4–0.9 mSv/year to 0.25–0.55 mSv/year, corresponding to a reduction of about 1.5–1.6 times.

As a result, the total annual effective dose received by workers decreased from an initial range of 1.2–2.7 mSv/year to 0.75–1.65 mSv/year after treatment. These values are significantly lower than the permissible limit of

20 mSv/year established by regulatory standards, indicating a low level of radiation risk to workers' health.

Thus, the proposed soil treatment methodology enables effective control of radiation risk factors in mining enterprises, reduces occupational radiation exposure, and improves working conditions. The obtained results confirm the practical significance of this technology within radiation safety systems and scientifically justify its implementation in industrial applications.

REFERENCES

- [1] A.A. Boboyev and all., Experimental-statistical models and algorithm for predicting the risk to workers' lives as a result of contamination of surface waters with radionuclides, Academy of the ministry of emergency situations of the Republic of Uzbekistan ISSN 2181-9327 No. 4 (21), 2025 ,Fire and explosion safety, scientific-practical electronic journal Tashkent – 2025
- [2] A.A. Boboyev, O.K. Mavlonov, M.M. Atokulova, Methodology for planning emergency evacuation from underground fires, Human capital and labor protection scientific-practical electronic journal Tashkent – 2025 ISSN. 3060–4982 No. 4 (7), 2025
- [3] A.M. Muzafarov, A.A. Boboev, R.R. Nurmatova, Progress issledovaniy po primeneniyu radona Rn 222 pri vzaimodeystvii podzhennyx i poverkhnostnyx vod, Protecting human capital and labor, scientific and practical electronic journal Tashkent - 2025 ISSN. 3060–4982 № 4 (7),
- [4] A.M.Hojiev, T.V.Botirov, Sh.B.Latipov, A.A.Boboev, Algorithms for improving the safety of working conditions of workers in underground mining operations, risk factor assessment, Human capital and labor protection, scientific–practical electronic journal Tashkent – 2025 ISSN. 3060–4982 № 4 (7), 2025
- [5] Timofeeva S.S., Boboev A.A., Timofeev S.S. Assessment of occupational risks in the mining and extraction of gold from the ores of Murantau deposit // Mining Bulletin of Uzbekistan. - Navai, 2020, No. 2 (81), P.107 - 111
- [6] Timofeeva S.S., Musaev M.N., Drozdova I.V. Boboev A.A., Assessment of occupational risks of workers engaged in open-pit mining // Development of science and technology - Bukhoro, 2020, No. 6, C 293 - 301
- [7] Timofeeva S.S., Drozdova I.V., Boboev, A.A. Assessment of occupational risks of employees engaged in open-pit mining // E3S Web of Conferences 177, 06006. Ural Mining Decade 2020, <https://doi.org/10.1051/e3sconf/202341704006>
- [8] Timofeeva S.S., Timofeev S.S., Boboev A.A. Phytoremediation potential of aquatic plants of Uzbekistan for treatment of cyanide-containing wastewater // International Conference on Construction, Architecture and Technosphere Safety. Conference Series IOP: Materials Science and Engineering, Russia. - Sochi, Vol. 962, 6 - 12 September 2020.
- [9] Boboev A.A., Allaberganova G.M. General properties of ionizing radiation and assessment of the magnitude of technogenic impact on the environment // Science and technology development - Bukhara, 2021 No. 1, 262 -266 p.
- [10] Timofeeva S.S., Musaev M.N., Boboev A.A., Monitoring to reduce radioecological impact on the environment // Nukus State Pedagogical Institute named after Ajinyoz, ILIM and JAMIYET Scientific and methodological journal 2021, No. 4 44 - 45 p.
- [11] Timofeeva S.S., Musaev M.N., Botirov T.V. Boboyev A.A., Mathematical models and algorithms for predicting surface water pollution // International Scientific Journal Theoretical & Applied Science. - Volume 104, Issue: 12, - December, 2021. - pp.1038 - 1042 (GIF 3))
- [12] Muzafarov A.M., Boboev A.A. Radioecological factors and methods of their determination in uranium technogenic objects // XXI century. Technosphere safety. - Irkutsk, 2020. - #3 (19). - S. 330-336
- [13] S. Timofeeva, G. Smirnov, A. Boboev and O. Goziev Use of artificial intelligence to prevent spontaneous combustion of coal E3S Web Conf. Goziev Use of artificial intelligence to prevent spontaneous combustion of coal E3S Web Conf., 417 (2023) 04006 DOI: <https://doi.org/10.1051/e3sconf/202341704006>
- [14] A.G. Vakhromeev, A.A. Boboev, N.N. Namozov, Sh. Namozov, Sh. Khushvaqtoev. Geoecological monitoring of the "Mustaqillikkin 25 uilligi" gas field E3S Web Conf. 417 04007(2023) DOI: <https://doi.org/10.1051/e3sconf/202341704007>
- [15] Development of safe products from local waste of oil and fat production Dilnoza Rakhmatova, Matrufjan Musaev, Gulnora Gulomova, Malika Aripkhadzhaeva, Dilrabo Nizamova E3S Web Conf. 371 01035 (2023) DOI: 10.1051/e3sconf/202337101035 "A 'layman's' explanation of Ultra Narrow Band technology," Oct. 3, 2003. [Online]. Available: <http://www.vmsk.org/Layman.pdf>. [Accessed: Dec. 3, 2003].
- [16] Dolchinkov N. , Investigation of the State of the Radiation Control Systems and the Actions of the Competent Authorities and the Population in the Event of a Change in the Radiation Background in Bulgaria, International conference KNOWLEDGE-BASED ORGANIZATION Subuy, Romania 24(3): p.38-44
- [17] Dolchinkov N., N. Nichev, Gamma-background radiation control systems as a factor of Bulgaria's national security, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume IV, Print ISSN 1691-5402, Online ISSN 2256-070X, <https://doi.org/10.17770/etr2024vol4.8225>, pp 83-88
- [18] Dolchinkov N. and N. Nichev, Structure and Management of the National Automated System for Permanent Control of the Radiation Gamma Background in Bulgaria, De gruyter open, Land Forces Academy Review Vol. XXII, No 2(86), 2017, Sibiu, Romania, p 115-121.
- [19] Dolchinkov N. , Historical overview and analysis of national automated system for continuous monitoring of gamma radiation, VIII науково-практичного семінару з міжнародною участю "Економічна безпека держави і науково-технологічні аспекти її забезпечення", Київ, 21-22 жовтня 2016 року ISBN 978-966-7166-38-0 p. 220.228
- [20] L. Lazarov, General Terms and Conditions for the Radio Connection Jamming, International Conference on High Technology for Sustainable Development, HiTech 2018 - Proceedings, 2018, 8566645
- [21] Stefanova, D.P., Vasilev, V.P., Efremovski, I.P. (2023). Re-Innovative Organizational Design: Sustainable Branding and Effective Communication - Applied Models in a World With New Borders/Without Borders;; Book Chapter: Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing, pp. 112–127; <https://doi.org/10.4018/978-1-6684-8681-8.ch006>; <https://www.igi-global.com/gateway/chapter/325452#pnlRecommendationForm>
- [22] Todorov, D.N., State of the population disclosure systems in the changing radiation situation in Bulgaria, Vide. Tehnologija. Resursi - Environment, Technology, Resources, 2019, 1, pp. 54–58
- [23] Dolchinkov N., Modernization of monitoring and public notification systems in case of radioactive pollution of the environment in Bulgaria, Scientific and Practical Journal "Global Nuclear Safety", No. 3 (24) 2017, Moscow, MEPI, Russia, p 7-18. Available: <https://www.researchgate.net/publication/321905753>
- [24] Dolchinkov N., Optimization of the systems for monitoring and public disclosure of radioactive contamination of the environment,International journal „Knowledge “, Skopie ISSN 1857-92 Vol 15.1 p. 423-431 GIF 1.023 (2015) . Available: <https://www.researchgate.net/publication/320378173>
- [25] Vambol S., N. Dolchinkov, V. Vambol, S. Abbas, S. Yermenko, O. Trush, Mathematical modeling study of the process of transfer radioactive contamination from the Chernobyl accident zone, Journal of Mountain Area Research, ISSN: 2518-850X (Online), 2518-8496 (Print), 2024
- [26] Dolchinkov N., Optimizing energy efficiency in the conditions of a global energy crisis, Optimizing Energy Efficiency During a Global Energy Crisis, 2023, ISBN13: 9798369304006 EISBN13:

9798369304013, <https://doi.org/10.4018/979-8-3693-0400-6> pp. 1–9.

- [27] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Improvement of Constructive-Technological Approaches Reducing Innovative Obsolescence of Industrial Technologies in the Context of Industry 4.0, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 180–186.
- [28] Petrova, D., Vlahova, B., Lengerov, A., Zlateva-Petkova, T., Study of the State of Innovation Development and Obsolescence in the Republic of Bulgaria of Companies from the Mechanical Engineering Sector, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2023, 1, pp. 187–194.
- [29] Petrova, D., Innovative Obsolescence in Mechanical Engineering and Singleness of Indicators, Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 2024, 3, pp. 221–224.
- [30] Toneva, D., Dimitrova, D., Some aspects of the water crisis in Bulgaria, 5th International Scientific Practical Conference „Environment. Technology. Resources “, Published by Rezekne Academy of Technologies, Latvia. Volume I, pp. 373-377, ISSN 1691-5402, ISBN 978–171389957–0..

Analysis of the Human Body Positioning in Disaster Remediation

Svilen Neykov

Bulgarian Defence Institute
“prof. Tsvetan Lazarov”
Sofia, Bulgaria
svilen@nkv.me

ORCID: [0009-0005-3975-2781](https://orcid.org/0009-0005-3975-2781)

Rosen Iliev

Bulgarian Defence Institute
“prof. Tsvetan Lazarov”
Sofia, Bulgaria
r.iliev@di.mod.bg

Abstract—The paper presents an approach to detection, classification and decision making for disaster relief scenarios, based on imaging data, pose estimations, depth perception and scene understanding, utilizing AI while performing on low power hardware.

Keywords— AI, detection, classification, disaster relief, pose estimations, low power hardware.

I. INTRODUCTION

Disaster remediation is one of those spheres that sit on the line between the military and the civilian space, as it is not a prime directive of the army to assist in these situations, but usually they are the ones with the most suitable equipment to lend a hand. As such, the armed forces of each nation should be interested in the most up-to-date ways to verify where their efforts will be the most valuable – which is where the chance to save a human life is.

Here we come to the most pressing issue – in a disaster remediation mission we can assume that there are victims in the whole region, but where would we find the ones that are most in need of assistance.

In this paper, we will address this question and propose a way to observe and evaluate where the disaster relief forces must concentrate their efforts in order to mitigate potential loss of life.

II. MATERIALS AND METHODS

Both through Geo-political tensions rising and changes to the climate of the planet, disaster relief becomes more important with each passing day. One of the pillars in this is the localisation of impacted people in the area of the disaster.

With the advancement of technology this aspect can be off-loaded from ground-based search parties and aerial

observers on planes/helicopters to a lot more mobile platforms, such as UAVs, UGVs and USVs.

The most perspective platform we can use for fast deployment and detection is the UAV, as aerial photography provides information for a very wide area. However, this now thrusts the responders onto the next hurdle – these platforms have a very limited carrying capacity for sensors, fuel/batteries and in general computational capabilities. This necessitates that the industry and researchers to develop more efficient algorithms that will be loaded unto these platforms.

A. Object Detection and Classification

As a visual animal, we perceive most of the world around us through sight. Our sight is sharp, but it relies on cues, movement, patterns and imperfections. However, as we are prone to boredom, tiredness and in general loss of sight, we are increasingly more reliant on the “digital eye”.

Sensors are our solution to the imperfections of the human eye and psyche. They can process information faster and can be adapted to a far greater extent to varying conditions. Thus, we have Computer Vision.

Computer Vision has a wide range of applications, from industrial applications for defect detection, sorting, maintenance, etc. through healthcare, by tumour detection, blood cell counting, etc., everyday applications such as licence plate reading for parking lot entry or highway control to the vast military domain.

One of the major computer vision aspects is Object Detection and Classification. Traditionally object detection has utilized sliding windows which select regions of the image, but it is very hard to find the optimal number of these windows. The traditional methods rely heavily on manually created features, which struggle with accuracy and robustness when viewing diverse objects and possess complex backgrounds. These features also have one additional flaw -they are not universal; this translates to

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.149>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

poor multi-domain performance and high complexity and time-consumption in region selection. With Deep Learning (DL) booming in the industry, object detection utilizing DL has vastly improved and surpassed traditional object detection methods. DL-based algorithms use very intricate and strictly hierarchical architectures; these enable the training of more complex features. Also, owing to the significant learning capabilities of convolutional neural networks (CNNs) feature can be better represented than traditional methods. This in turn raises significantly the robustness and eliminates the manually created features. [1]

B. Pose Estimation

Pose estimation is a subset of the computer vision task that is to detect human key joints from general data sets. It is an important task in computer vision, skeleton-based action recognition can be based on its results to determine the type of motions. [2]

In this context the poses that are most likely to be of interest to the researcher or the people in the field is if you can detect an anomalous position of the body or extremities, which will signal the need for intervention.

C. Scene Understanding

Scene understanding in the context of Computer Vision is the Analysis of the frame as a whole, where apart from the detection, classification and pose estimation the disaster remediation teams or researchers need to know, not only if there is a person that is in need of assistance, but what are the conditions around him, is it viable to send help, what kind of risk is involved, or in short, what kind of help is needed.

D. UxVs

The use of multiple unmanned vehicles in recent years has skyrocketed. From the war in Ukraine and the incidents in the Baltic Sea we can see that the face of any conflict has changed significantly in the use of such platforms. Disaster relief is also not a stranger to these changes; multiple platforms are being developed and introduced:

- DJI Matrice 4TD / 4T (2026 Model): Recognized as a premier choice for 2026, offering 640×512 thermal imaging, 56× optical zoom, and IP55 weather resistance, allowing it to operate in rain, snow, and strong winds.
- Autel Robotics EVO Max 4T: Specialized for SAR with dual thermal sensors, 42-minute flight endurance, and 15km transmission range, making it ideal for large, complex search areas.
- Skydio X10: Highlights advanced AI for obstacle avoidance and autonomous flight paths, minimizing operator workload in dense urban or mountainous areas.
- WingtraRay (VTOL): Combines vertical takeoff and landing with fixed-wing

endurance, capable of covering up to 350 square kilometers per mission, ideal for large-area wilderness searches.

- GDU UAV-P300: Introduced at CES 2026, this FPV drone features AI-powered "fog-penetrating" optical, electronic, and AI de-fogging tech for operation in poor weather.
- DJI Dock 3 (Drone-in-a-Box): Enables automated 24/7 deployment, where a drone automatically takes off, scans a pre-programmed area, and returns to charge without human intervention, ideal for rapid initial response.[3][4]

For the trends in UxVs we can see that the most vital areas are:

- AI-Enhanced Detection: AI algorithms distinguish human heat signatures from environmental heat sources (e.g., fires) in thermal data, increasing success rates.
- Thermal/Multispectral Integration: Drones are frequently carrying combined thermal, zoom, and RGB cameras to identify victims in low-light, fog, or through light foliage.
- Automatic 3D Mapping: Drones can generate real-time 3D models of destroyed structures, allowing responders to identify safe entry points.
- Fiber-Optic Data Links: To fight electronic warfare and signal jamming, new drones are using fiber-optic cables for secure, high-definition data transmission.[5]

With all of the aspects discussed above, the combination of which can lead to a greater development in the Disaster Relief systems and strategies that all countries need to address.

III. RESULTS AND DISCUSSION

A. Setup

Utilizing state-of-the-art algorithms, we can assess all of the points in this paper, as one of the leading directions for development of detection models is bringing them to edge applications, therefore minimizing their resource footprint. [6]

1) The Model: One such model is the evolution of the YOLO (You Only Look Once) family of models, this is a popular series of state-of-the-art, real-time object detection systems designed for high speed and accuracy. Unlike traditional two-stage detectors (like R-CNN) that first find potential object areas and then classify them, YOLO treats object detection as a single regression problem, directly predicting bounding boxes and class probabilities from full images in a single evaluation. The used model here is the new YOLO26. The performance improvements can be see in Fig.1 and Fig.2. There we can see the improvements that the new architecture, Fig.3 brings despite the lowering of the hardware

requirements.[6][7] One of the key features is that we can also use the same architecture for all 3 major tasks ahead: Detection, Classification and Pose Estimation.

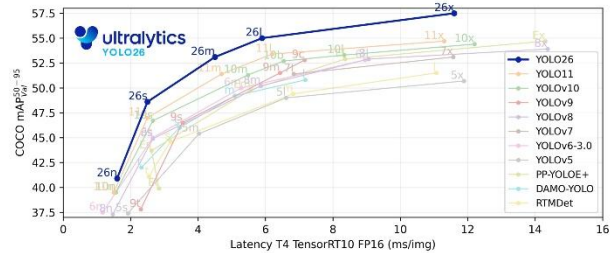


Fig. 1. Performance improvement of YOLO26. [6][7]

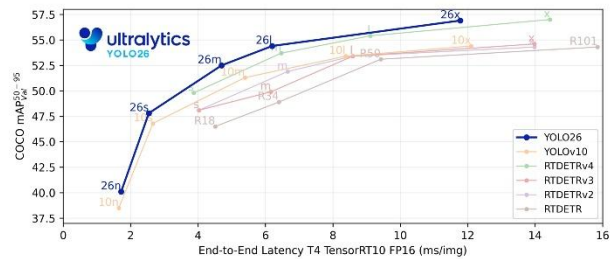


Fig. 2. E2E Performance improvement of YOLO26. [6][7]

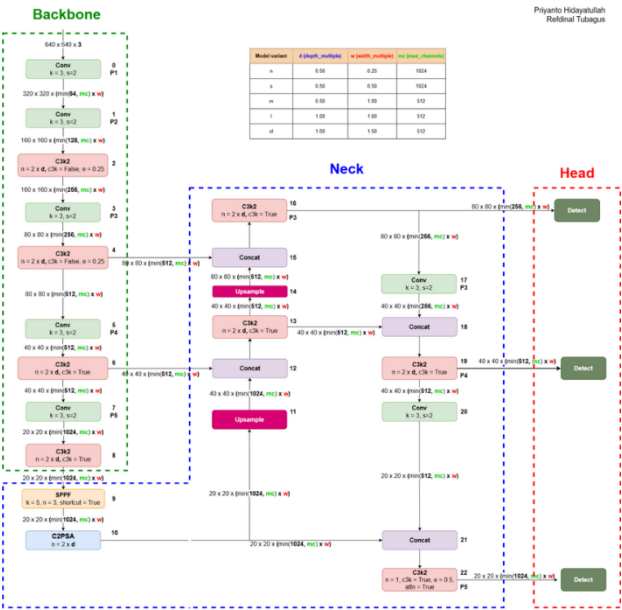


Fig. 3. Architecture of YOLO26. [7]

In the following tables we present the key performance indicators of the model used:

TABLE 1 YOLO26 DETECTION KPIS [6][7]

Model	size	mA pval	mA pval	Speed	Speed	par ams	FL OPs
	(pix els)	50-95	50- 95(e2e)	CPU ONN X	T4 Tensor RT10	(M)	(B)
				(ms)	(ms)		
<u>YOLO O26n</u>	64 0	40.9	40.1	38. 9 ± 0.7	1.7 ± 0.0	2.4	5.4
<u>YOLO O26s</u>	64 0	48.6	47.8	87. 2 ± 0.9	2.5 ± 0.0	9.5	20.7
<u>YOLO O26m</u>	64 0	53.1	52.5	220 .0 ± 1.4	4.7 ± 0.1	20.4	68.2
<u>YOLO O26l</u>	64 0	55	54.4	286 .2 ± 2.0	6.2 ± 0.2	24.8	86.4
<u>YOLO O26x</u>	64 0	57.5	56.9	525 .8 ± 4.0	11.8 ± 0.2	55.7	193. 9

TABLE 2 YOLO26 CLASSIFICATION KPIS [6][7]

Model	size	ac c	ac c	Speed	Speed	para ms	FL OPs
	(pix els)	top 1	top 5	CPU ONN X	T4 Tensor RT10	(M)	(B) at 224
				(ms)	(ms)		
<u>YOLO 26n-cl</u> s	22 4	71 .4	90 .1	5.0 ± 0.3	1.1 ± 0.0	2.8	0.5
<u>YOLO 26s-cl</u> s	22 4	76	92 .9	7.9 ± 0.2	1.3 ± 0.0	6.7	1.6
<u>YOLO 26m-cl</u> s	22 4	78 .1	94 .2	17. 2 ± 0.4	2.0 ± 0.0	11.6	4.9
<u>YOLO 26l-cl</u> s	22 4	79	94 .6	23. 2 ± 0.3	2.8 ± 0.0	14.1	6.2
<u>YOLO 26x-cl</u> s	22 4	79 .9	95	41. 4 ± 0.9	3.8 ± 0.0	29.6	13.6

TABLE 3 YOLO26 POSE KPIS [6][7]

Model	size	mA ppose	mA ppose	Sp ee d	Spe ed	par ams	FL OP s
	(pix els)	50- 95(e2e)	50(e2e)	CPU ON NX	T4 Tensor RT10	(M)	(B)
				(ms)	(ms)		
<u>YOL O26n- pose</u>	64 0	57.2	83.3	40. 3 ± 0.5	1.8 ± 0.0	2.9	7.5
<u>YOL O26s- pose</u>	64 0	63	86.6	85. 3 ± 0.9	2.7 ± 0.0	10.4	23. 9
<u>YOL O26m -pose</u>	64 0	68.8	89.6	21 8.0 ± 1.5	5.0 ± 0.1	21.5	73. 1
<u>YOL O26l- pose</u>	64 0	70.4	90.5	27 5.4 ± 2.4	6.5 ± 0.1	25.9	91. 3
<u>YOL O26x- pose</u>	64 0	71.6	91.6	56 5.4 ± 3.0	12.2 ± 0.2	57.6	201 .7

As our focus is on edge applications and low-powered hardware, we will be using the n and s variants.

2) *The Dataset*: One of the biggest challenges in both the military and the disaster relief fields of study as always is the available datasets for training and development of appropriate models and pipelines. Especially as such, when we are trying to view different poses. Fortunately there are examples of such datasets that can be used, one such dataset is the C2A Dataset: Human Detection in Disaster Scenarios [8]. The C2A (Combination to Application) Dataset is a resource designed to advance human detection in disaster scenarios using UAV imagery. This dataset addresses a critical gap in the field of computer vision and disaster response by providing a large-scale, diverse collection of synthetic images that combine real disaster scenes with human poses. This dataset combines sources such as the Aerial Image Dataset for Emergency Response Applications (AIDER) and the human poses derived from the Multiple Poses Human Body (LSP/MPII-MPHB) dataset. Key features include:

- a) 10,215 high-resolution images
- b) Over 360,000 annotated human instances

c) 5 human pose categories: Bent, Kneeling, Lying, Sitting, and Upright

d) 4 disaster scenario types: Fire/Smoke, Flood, Collapsed Building/Rubble, and Traffic Accidents

e) Image resolutions ranging from 123x152 to 5184x3456 pixels

f) Bounding box annotations for each human instance

Examples of these can be seen in Fig.4-6.



Fig. 4. Example of detection in C2A dataset. [8]



Fig. 5. Example of augmented image in C2A dataset. [8]



Fig. 6. Example of augmented image in C2A dataset. [8]

B. Results

We created a three-branch pipeline for posture classification in order to compare different ways of extracting discriminative information from the same input images. This was motivated by the fact that posture recognition can depend on global appearance and on local body configurations, therefore it is not optimal to have a single representation in all cases.

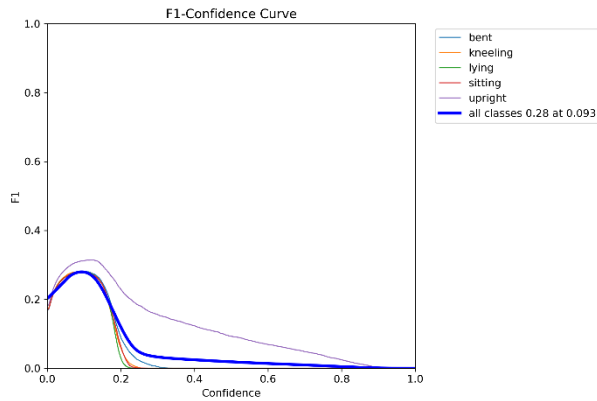


Fig. 7. F1 curve for Branch 1.



Fig. 8. Branch 1 Confusion Matrix.

1) Branch 1: Direct image-based detector, which had a role of providing a baseline, using the full visual context of the image. This included the silhouette, orientation and scene-level cues. This was expected to be the most robust one, as it does not depend on intermediate pose estimations and exploits all of the available visible discriminative information.

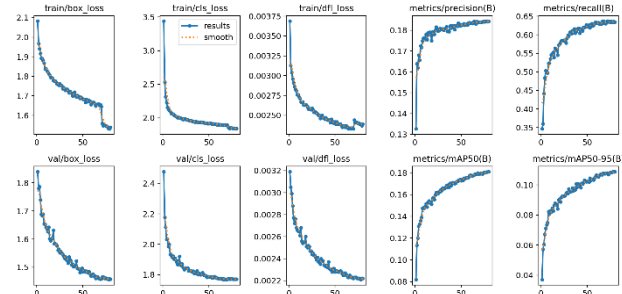


Fig. 9. Branch 1 results

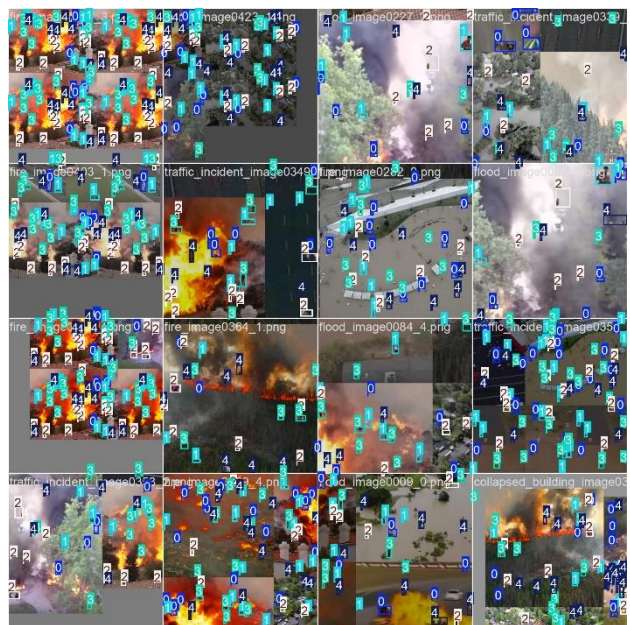


Fig. 10. Branch 1: Training Batch



Fig. 11. Branch 1: Validation batch, labels



Fig. 12. Branch 1: Validation batch, predictions

2) *Branch 2:* This was designed around keypoints extracted from the entire image. The main idea was that an explicit pose representation may improve classification by applying a focus on the structure of the body, not on appearance. In practice, the full-image formulation introduced too much irrelevant context and did not isolate the person tightly enough. This significantly reduced the usefulness of the keypoint signal.

3) *Branch 3:* Here we used keypoints that were extracted from a cropped, more localized region of the image, centred on the identified person. Here we wanted to preserve the benefits of pose-based reasoning while reducing the background noise and to improve the concentration of the pose signal. This resulted in the most promising pose-based formulation, because it retained more useful information, compare to the full-image branch.

Head-to-head branch wins by class (latest test run)

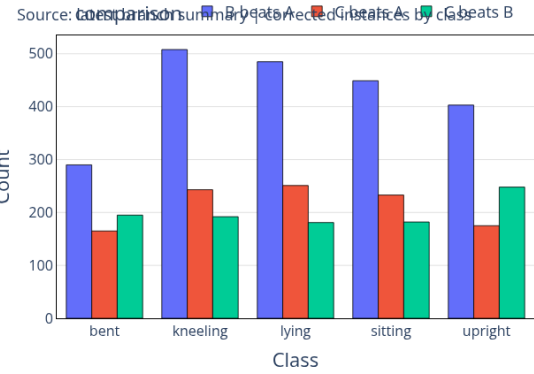


Fig. 13. Branch wins by class

Per-class accuracy by branch (latest test run)

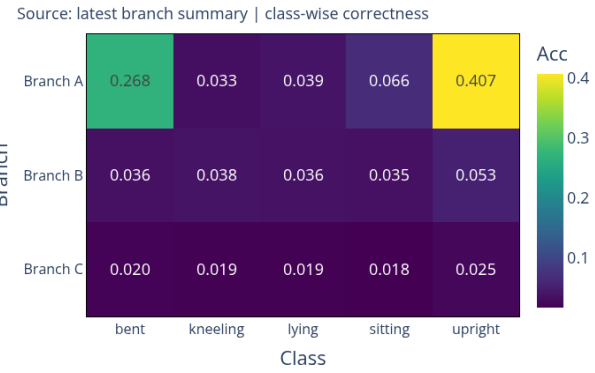


Fig. 14. Heatmap between the branches

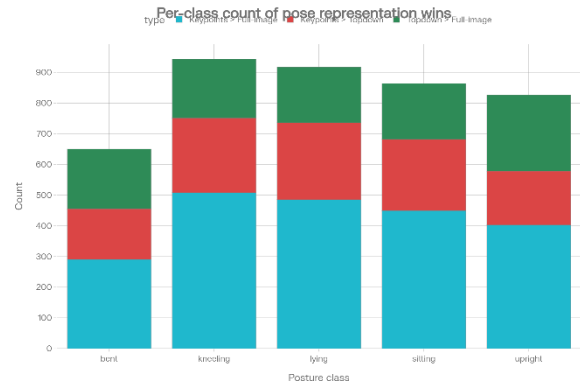


Fig. 15. Per-class wins

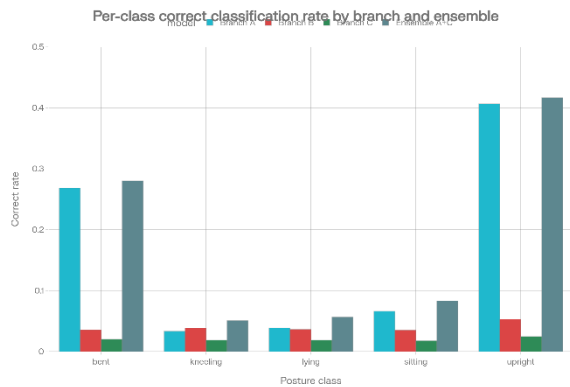


Fig. 16. Per-class rates

During the experimentation, we came to the conclusion, that the original full image keypoint branch was not providing a sufficient signal, the pipeline had to be changed in order to perform the extraction on a more localized crop rather than on the entire image. This improved the pose input and the whole branch was more interpretable.

An adjustment was made also to the evaluation strategy, so that it better reflects the complementary behaviour of the branches. Instead of presenting them as equal model candidates, we treat the direct detector as the primary reference method, the crop-based keypoint branch as the main pose-based method, and the full-image branch as an ablation showing the limitations of the original pose formulation.

Blood Detection is also very important in disaster relief scenarios. As such, a optional detector focusing on this was trained as well. It performs really well as seen in the figure 17.

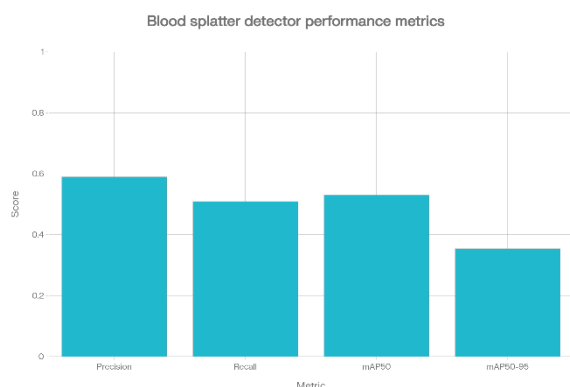


Fig. 17. Blood splatter metrics

It can be a very useful addition to the pipeline, as long as the other branches are performing as expected, as this can be a major decision making indicator.

C. Discussion

The main finding is that appearance-based detection remains as the most reliable approach, while pose-based classification becomes useful only after localization of the

input. This suggests that the critical factor was not the pose information, but the quality of the pose representation. When the region for the body is tightly cropped, the model preserved a more discriminative structure and produced better results compared to the full-image branch.

This shows us that the design of the pipelines and the branches within matters as much, or even more that the choice of the detection model. A pose branch can fail not because the pose does not provide enough information, but because the input is too noisy or too diluted by the background context. This is evidenced by the revised crop-based branch, and the improved performance after localization.

Future work should be focused on converting the current branch-level combinations to a true learned fusion framework. The natural next step is confidence-aware ensembling, where branch outputs are weighed according to prediction certainty or class-specific reliability. Other steps could include probability calibration for more comparable detector and pose branches before fusion; adding a meta-classifier, which can learn when to trust each branch, this will probably outperform the fixed logic.

ACKNOWLEDGMENT

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. D01-74/19.05.2022.

REFERENCES

- [1] Yibo Sun and Zhe Sun and Weitong Chen, The evolution of object detection methods <https://www.sciencedirect.com/science/article/pii/S095219762400616X>, 2024. <https://doi.org/10.1016/j.engappai.2024.108458>
- [2] Rujing Yue, Zhiqiang Tian, Shaoyi Du, Action recognition based on RGB and skeleton data sets: A survey <https://www.sciencedirect.com/science/article/abs/pii/S0925231222011596>, 2022, <https://doi.org/10.1016/j.neucom.2022.09.071>
- [3] Best Drone for Search and Rescue: Emergency Response Drones for Teams, [Online]. Available: <https://www.flybyguys.com/blog/drones-for-search-and-rescue>
- [4] New AI-powered fog-penetrating first responder drone debuts at CES 2026, [Online]. Available: <https://aerospaceglobalnews.com/news/ai-powered-search-rescue-drone-ces-2026/#:~:text=New%20AI%2Dpowered%20fog%2Dpenetrating,support%20search%20and%20rescue%20operations.&text=GDU%20says%20its%20new%20UAV,offers%20significantly%20improved%20imaging%20capabilities.>
- [5] Emergency and Rescue Robot Market, [Online]. Available: <https://www.intelmarketresearch.com/emergencyrescue-robot-market-26181#:~:text=Startups%20like%20Unitree%20Robotics%20are,and%20Rescue%20Robot%20Market%20Trends>
- [6] Glenn Jocher and Jing Qiu, Ultralytics YOLO26, [Online]. Available: <https://github.com/ultralytics/ultralytics>
- [7] Priyanto Hidayatullah, Refdinal Tubagus, YOLO26: A Comprehensive Architecture Overview and Key Improvements https://www.researchgate.net/publication/400855947_YOLO26_A_Comprehensive_Architecture_Overview_and_Key_Improvements, 2026.

- [8] Ragib Amin Nihal, Benjamin Yen, Katsutoshi Itoyama, and Kazuhiro Nakadai, UAV-Enhanced Combination to Application: Comprehensive Analysis and Benchmarking of a HumanDetection Dataset for Disaster Scenarios, <https://arxiv.org/pdf/2408.04922>, 2024

Assessment of the Applicability of International Frameworks and Standards for Cybersecurity as a Basis For Building a Classification Model in the “Security and Defence” Sector

Atanas Nikolov

Defence Institute “Prof. Tzvetan Lazarov”

Sofia, Bulgaria

a.nikolov@di.mod.bg

Abstract— The report presents an analysis of leading international cybersecurity standards and frameworks to assess their applicability in building a cyber-incident response model at the political, strategic, operational and tactical levels. The emphasis is on examining the vertical and horizontal connections between the individual levels and standards, as well as on identifying the opportunities and limitations of the standards/frameworks.

Keywords — Cybersecurity, standard, framework, multidimensional model.

I. INTRODUCTION

Cyberspace is characterized by an ever-increasing malicious activity by groups carrying out targeted attacks, including Advanced Persistent Threat (APT) attacks. These groups are often sponsored by state/government organizations, use a variety of techniques, and despite (almost continuous) documentation of these techniques and tactics, the information available about them often remains insufficient, and in many cases almost non-existent. This makes it difficult to formulate reliable conclusions, achieve real awareness, or make the right decisions. Analysing the frequency, interrelationships, and context of the used techniques/tactics provides a basis for a better understanding of how attackers shape and escalate their actions.

In terms of cybersecurity, many standards and frameworks have been created, such as: MITRE ATT&CK/D3FEND, STIX/TAXII, ISO 27001, NIST SP 800-61, CAPEC, Cyber Kill Chain or others, and they all address different aspects of cybersecurity [1], [2], [3]. On the one hand, they complement or overlap and solve problems at certain levels, but on the other hand, their applicability in certain cases is limited. In other words, there is no comprehensive mechanism that can provide

understanding, management and approach to protection in cyberspace. In this context, this report proposes a model for structuring knowledge based on international standards and frameworks and on this basis introduces a multi-layered structure that covers the political, strategic, operational and tactical levels, and defines a mechanism for interaction both vertically and horizontally.

II. EXISTING CLASSIFICATION MODELS IN THE CONTEXT OF CYBERSECURITY

As cyberthreats evolve, classification models have evolved from static, incident-oriented approaches to dynamic, adaptive, and multidimensional models. This trend is naturally dictated by the need to promptly take adequate measures (detection, analysis, and incident response) and by the constantly increasing volume and complexity of attacks.

The first approaches are based on static standards/frameworks that define a set of controls and good practices. This group includes standards such as ISO/IEC 27001 [3], early versions of the NIST Cybersecurity Framework [4], etc., and despite their limited adaptability to modern threats, these standards and frameworks provide a basis for security management and the creation of behavioural and contextual models that are based on observation and analysis of the behaviour of various objects (users, systems, and network devices, etc.). They are based on the concept of a “baseline” and any anomaly/deviation from this level is a prerequisite for “raising” an alarm. In this way, the efficiency in detecting new attacks increases.

In taxonomies based on tactics, techniques and procedures (TTPs), a relatively in-depth analysis of the attacker’s behaviour can be performed, which allows for a

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.84>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

detailed analysis of cyberattacks. This group includes standards and frameworks such as MITRE ATT&CK, CAPEC and Cyber Kill Chain [1], [5], [6], which provide structured models for analysing the behaviour of the adversary/attacker and the life cycle of the attack. In practice, they achieve systematization of knowledge about attacks, which on the one hand facilitates the analysis of incidents, and on the other hand supports the development of adequate response mechanisms. The integration of these models with Threat Intelligence represents the next step in the evolution of classification approaches, and their connection with real indicators of compromise and/or campaigns builds the next level of awareness, which in turn provides an opportunity for proactive protection, especially in environments with increased requirements for rapid response, such as the "Security and Defence" sector.

Almost simultaneously with the development of these models, the trend toward automation and the use of machine learning is also increasing, which allows the use of automated systems for processing, analysis and response. The evolution of these approaches leads to the formation of multidimensional and layered models, which now combine different characteristics of cyber incidents. In practice, these models represent the complex nature of modern threats, in which each event is considered not in isolation, but as part of a larger process with multiple interconnected stages.

Despite the diversity of models and frameworks, they all consider separate aspects of cybersecurity and are oriented towards specific application levels. This reinforces the thesis that there is no integrated approach that ensures connectivity between the different levels "from political and strategic to operational and tactical" and a mechanism for coordination between the individual standards. Separate consideration limits their effectiveness in building complex protection systems and making informed decisions.

III. CYBERSECURITY STANDARDS AND FRAMEWORKS

This report examines a total of 19 cybersecurity frameworks and standards, which are positioned at different organizational levels, addressing different aspects of cybersecurity. This allows for a clear definition of their role and scope of application. This provides a basis for a better understanding of the interrelationships between them and for building a comprehensive model.

Frameworks such as NIS2, ENISA and NATO CCDCOE set normative requirements that are more of a national, allied or regulatory nature. This makes them suitable for national planning, cybersecurity policy-making and coordination, but not for organizing technical activities [7], [8], [9].

Next, frameworks and standards such as NIST CSF, ISO/IEC 27001 and ISO/IEC 27002 introduce risk management, organizational maturity, resilience, critical infrastructure, audit, detection, response and recovery functions, which emphasizes their role as a coordinator in cybersecurity. For this reason, requirements for information security management systems and auditing are also defined here, but they do not provide a mechanism for

analysing attacks, processes or destructive behaviour, and are limited in terms of quantitative risk assessment [3], [4], [10].

The main strength of NIST SP 800-61, ISO/IEC 27035 and VERIS is in the organization of activities, reporting and analysis of events, documentation, incident management. This gives them a central place in the operational management of cybersecurity, and despite their strong operational response, these standards do not provide a behavioural taxonomy of attacks and do not define techniques, tactics, and procedures necessary for detailed analysis, protection, and assessment of the effectiveness of measures [11], [12], [13].

The latter group of standards and frameworks is of key importance for the technical aspects of cybersecurity and structured information exchange. The first subgroup focuses on the analysis of attacker behaviour, techniques, tactics, and procedures, vulnerabilities, protection measures, indicators, and response. This includes standards and frameworks such as MITRE ATT&CK, CAPEC, Cyber Kill Chain, Diamond Model of Intrusion Analysis, MITRE D3FEND, CVE, NVD and CVSS, which define behavioural taxonomies, provide analytical description and modelling, define attack phases, define defence measures, and despite their strong analytical functions and integration with specialized platforms, they are not intended for incident management or information exchange [1], [2], [5], [6], [14], [15], [16], [17]. The second subgroup includes standards and frameworks such as STIX and TAXII, which specialize in the structured description and exchange of information about attacks, techniques, tactics, procedures, indicators of compromise and the relationships between them. Despite their weak analytical and management functions, they make a significant contribution to ensuring compatibility and coordination both horizontally and vertically [18], [19].

The analysis shows that the standards and frameworks considered cover different aspects of cybersecurity. For this reason, they remain fragmented in terms of their application and although each standard or framework can be attributed to a different problem, and hence to a different level, it can be argued that it is impossible to achieve complete integration with the other levels and standards or frameworks. This necessitates the creation of a mechanism that connects the analytical, management and technical components into a coherent and coordinated structure. This model must be able to ensure coherence between the levels, define interrelationships and support the effective use of standards and frameworks in complex environments.

IV. METHODOLOGY FOR ASSESSING APPLICABILITY

When analysing and comparing standards and frameworks, the application of predefined criteria is a necessary condition for achieving methodological soundness. The lack of a clear assessment framework leads to a fragmented analysis, in which individual standards are considered in isolation, without the possibility of structured comparison and drawing generalized conclusions. Such a criteria-oriented approach is widely used in research

methodology [14], [20], as well as in the specialized literature on risk and security management [21].

In this report, the assessment of the effectiveness and applicability of international standards and frameworks is carried out using criteria covering technical, operational and strategic aspects. Such a consideration facilitates not only an objective assessment, but also the identification of potential gaps and opportunities for adaptation and synchronization between different standards, frameworks and practices in cyberspace. These criteria are:

- **focus and scope** - determine which aspects of cybersecurity and incidents are covered and to what extent. The criterion describes whether the framework/standard is focused on specific technical categories (e.g.: vulnerability, TTP, IoC), on the overall incident lifecycle, or on risk management. In the context of the “Security and Defence” sector, this criterion is particularly important because it determines whether the framework can be applied to protect critical infrastructure, military networks, and/or hybrid operations;

- **degree of formalization** - indicates the extent to which the framework or standard uses clear, unambiguous definitions, unique identifiers, and structured categories for classifying threats and incidents. Highly formalized frameworks facilitate automation and integration with analytics platforms such as SIEM, SOAR, EDR, and XDR. This ensures that data can be collated, correlated, and used for algorithmic processing and machine learning. In the “Security and Defence” sector, high formalization is of utmost importance for ensuring compatibility between national and international systems/organizations/partners and for supporting coordinated protective measures/mechanisms, where incorrect or ambiguous definitions can lead to delays or errors in the coordinated response;

- **integration with operating systems** - shows the extent to which the standard or framework can be implemented and used in real analytical and protective platforms, such as SIEM, SOAR, EDR and XDR. The high degree of integration allows for automated collection, correlation and processing of data for incidents, indicators and attack techniques, minimizing manual labour and the risk of human error;

- **risk assessment support** - assesses the ability of the standard or framework to provide mechanisms for quantitative and qualitative assessment of the risk associated with cyber threats, vulnerabilities and incidents. Structured assessment methods, such as CVSS for vulnerabilities or integration with Risk Scoring algorithms, allow for prioritization of incidents and optimal allocation of protection resources. For example, a high level of support for risk assessments by a standard or framework facilitates management and strategic decision-making by providing objective and standardized data on the impact of various threats;

- **adaptability** - measures the ability of a standard or framework to update and evolve in line with the dynamic cyber threat environment and technological changes. This includes adding new techniques, indicators, categories and risk assessment mechanisms without disrupting the overall structural consistency of the model. Highly adaptable

frameworks allow for rapid response to emerging threats while maintaining compatibility with already implemented operational systems and analytical platforms;

- **interoperability** - reflects the ability of a standard or framework to interact effectively with other standards, frameworks, platforms and processes. A high level of interoperability means that the data and categories defined in the framework can be used together with different information systems, analytical tools and operational platforms without requiring complex transformations or manual mapping;

- **operational applicability or compatibility** - indicates the extent to which the standard or framework is suitable for real-world use in operational processes, including planning, detecting, and responding to cyber incidents. High operational applicability is expressed in the framework's ability to provide practically usable categories, methods, and indicators that can be implemented in team procedures, training, and/or automated systems.

The combined consideration of these criteria provides an approach for the evaluation, selection and adaptation of international frameworks and standards and supports the construction of integrated, multidimensional models that combine technical information, operational procedures and strategic objectives. This creates a solid basis for subsequent analysis and comparison.

The assessment scores were assigned based on publicly available documentation, implementation guidance, integration capabilities, operational adoption and documented functionality of the analysed standards and frameworks. The evaluation remains partially qualitative due to the heterogeneous nature of the analysed models and the different organizational and technical contexts in which they are applied. The assigned scores therefore reflect a comparative analytical assessment rather than an absolute quantitative measurement.

For the purposes of the analysis, a scale (TABLE I) with three levels (scores: low, average and high) is used, which allows a standardized assessment of the degree of compliance of each framework/standard with the defined criteria.

TABLE I. RATING/COMPARISON SCALE

Score	Description
High (h)	- clearly defined and objectively documented in official standards or publications; - wide application to the relevant criterion;
Average (a)	- partial coverage of the criterion; - applicable in a specific context; - requires complementary frameworks or mechanisms;
Low (l)	- lacks or limited coverage of the criterion; - does not provide direct functionality;

V. APPLICABILITY/ANALYSIS

The analysis of the considered standards and frameworks is done through direct comparison in tabular form (TABLE II). The aim is to visualize their strengths, limitations and degree of applicability in the context of cybersecurity.

The comparison shows that the standards and frameworks are grouped into several groups. For example, frameworks with a high degree of formalization and integration (such as: MITRE ATT&CK, STIX/TAXII, CVE/NVD/CVSS) demonstrate high operational applicability and interoperability, which makes them suitable for use with automated analytical platforms. In contrast, frameworks such as NIS2, ENISA and NATO CCDCOE show a strong focus and scope, but limited direct integration with operational systems, which emphasizes their role at the strategic and political level.

TABLE II. COMPARATIVE ANALYSIS

№	Standard/ framework	Criteria						
		focus and scope	degree of formalization	integration with operating systems	risk assessment support	adaptability	interoperability	operational applicability or compatibility
1.	NIS2	h	h	l	a	a	a	l
2.	ENISA	h	h	a	h	h	h	a
3.	NATO CCDCOE	h	a	a	a	a	a	a
4.	NIST CSF	h	a	a	h	h	h	a
5.	ISO/IEC 27001	h	h	a	h	h	a	a
6.	ISO/IEC 27002	a	h	a	a	h	a	a
7.	NIST SP 800-61	h	h	a	a	h	a	h
8.	ISO/IEC 27035	h	h	a	a	a	h	h
9.	VERIS	a	h	l	a	h	a	a
10.	MITRE ATT&CK	h	h	h	a	h	h	h
11.	MITRE D3FEND	a	h	a	a	h	h	a
12.	CVE	a	h	h	l	a	h	h
13.	NVD	h	h	h	h	a	h	h
14.	CVSS	h	h	h	h	a	h	h
15.	CAPEC	a	a	a	a	a	a	a
16.	Cyber Kill Chain	a	l	l	l	l	a	a
17.	Diamond Model of Intrusion Analysis	a	a	a	l	a	a	a
18.	STIX	h	h	h	a	h	h	h
19.	TAXII	h	a	h	a	h	h	h

The comparative assessment should be interpreted as an analytical orientation framework intended to support multidimensional positioning and interoperability analysis rather than as a strict quantitative benchmarking mechanism.

In parallel, frameworks and standards such as NIST SP 800-61, ISO/IEC 27035, ISO/IEC 27001/27002 and NIST CSF occupy an intermediate position, providing a balance between formalization, risk management and operational applicability, but with limited integration with operational platforms, as they do not support machine processing mechanisms. In addition, models such as CAPEC, Cyber Kill Chain and Diamond Model provide in-depth analysis, but are limited in terms of automation and quantitative risk assessment. The table shows that CAPEC has uniform scores on all criteria, which on the one hand shows its balanced nature, but on the other hand also its limitations.

The analysis confirms the idea that there is no universal framework or standard that covers all criteria simultaneously. This necessitates the need for an integrated, multidimensional model that combines technical formalization, operational applicability and strategic focus, especially important for the "Security and Defence" sector.

VI. MODEL OF CONSIDERATION

Management in the "Security and Defence" sector is characterized by the distinction of tactical, operational, strategic and political levels, which function as a system for decision-making and coordination of actions. This model provides a transition from specifically implemented activities to strategic planning and formulation of national policies. Given that cybersecurity is considered as part of national security, the application of an analogous consideration is logically justified. In this regard, the positioning of the considered standards and frameworks relative to the relevant levels allows for an analysis of their capabilities and limitations, as well as determining their role and applicability within the model.

Of utmost importance for a model is to determine the "inputs" and "outputs" of the levels through which the transformation of technical data into strategic and political actions is carried out, and management decisions into operational and technical measures.

In the multidimensional model, the considered standards and frameworks can be positioned as follows:

- at the tactical level - MITRE ATT&CK, STIX, CVE, NVD, CVSS and partly MITRE D3FEND. These standards and frameworks have a high level of formalization, integration, machine processing and automation, which allows their direct use in operational systems such as SIEM, EDR and XDR. This level is the level for identifying incidents and implementing specific technical response measures;
- at the operational level - NIST SP 800-61, ISO/IEC 27035 and partly MITRE D3FEND, STIX and TAXII. High operational applicability, clarity and coordination capabilities allow the definition of management processes, coordination between teams and

tracking the incident life cycle. In this context, the STIX and TAXII standards support the standardized exchange and synchronization of information between systems and organizations;

- at the strategic level - NIST CSF, ISO/IEC 27001, ISO/IEC 27002 and ENISA. These standards and frameworks have a relative maturity in terms of risk management and integration with the management of the organization, which supports planning, prioritization and ensuring resilience. In practice, this level is where the linking of cybersecurity with strategic goals takes place. This is the level at which planning and management are implemented in the context of national policies;
- at the political level - NIS2, NATO CCDCOE and partly ENISA. These frameworks ensure compatibility and coordination at the international, allied level and have a strong connection with the regulatory framework. They define national and allied policies, regulatory requirements, which link cybersecurity with national security.

Another essential part of the multidimensional model are the vertical and horizontal interconnections, as follows:

- vertically - ensures the transformation of technical data into management decisions and the translation of strategic and political goals into specific actions;
- horizontally - ensures compatibility not only between different standards and frameworks, but also between organizational structures and technological environments. This is particularly important in the "Security and Defence" sector, where effective response to cyber incidents requires synchronization between national and allied systems, coordination between different institutions and work with classified information.

Vertical interconnections:

- from tactical to operational level - the generated technical data, such as indicators of compromise, the attacker's TTP, the generated logs and telemetry are structured using standards such as STIX, identified using CVE/NVD and analysed against MITRE ATT&CK. At the operational level, this information is used for correlation, aggregation and formation of incidents using NIST SP 800-61 and ISO/IEC 27035;
- from the operational level to the strategic level - information about events or group of events classified as incidents (including information about the scope, frequency, type of attack and effectiveness of protective mechanisms) are transmitted to the strategic level. Here they are used for risk assessment (including through CVSS scores generated at the tactical level), prioritization of measures and identification of trends. This is done within the framework of NIST CSF, ISO/IEC 27001 and ISO/IEC 27002;
- from the strategic to the political level - the summarized risk assessments, information about identified campaigns and/or system vulnerabilities are used to form strategic analyses and decisions. This interaction supports the development of policies and regulations within the framework of NIS2, as well as the definition of strategic guidelines developed by organizations such as NATO CCDCOE and ENISA;

- from political to strategic level – here policies, regulatory requirements and priorities are defined (e.g. through NIS2), which defines the framework for cybersecurity management. At the strategic level, policies are transformed into strategic objectives and risk management guidelines within the framework of NIST CSF and ISO/IEC 27001;

- from strategic to operational level – strategic priorities, acceptable risk levels, objectives and guidelines are transformed into specific requirements for operational structures. This includes defining processes, procedures and mechanisms for incident management according to NIST SP 800-61 and ISO/IEC 27035;

- from operational to tactical level – operational guidelines are implemented through specific technical measures (e.g.: detection rules, protection mechanisms or response scenarios), based on models such as MITRE D3FEND. These measures are implemented at the tactical level through integration with platforms such as SIEM, EDR and XDR, using data structured through STIX and TAXII.

Horizontal relationships:

- at the tactical level – behaviour (MITRE ATT&CK) is combined with specific vulnerability(s) (CVE/NVD), relevant priorities (CVSS), data format (STIX) and protection (MITRE D3FEND), as a result the attack is described by the technique used, vulnerability, risk, indicator and protection mechanism, which allows for real-time incident processing;

- at the operational level – processes are combined (NIST SP 800-61), management (governance), protection mechanisms (MITRE D3FEND) and formatted for exchange via STIX/TAXII. In this way, management, processing and formalized exchange of information about incidents is achieved;

- at the strategic level – risk management frameworks, control mechanisms and strategic guidelines are combined (NIST CSF, ISO/IEC 27001 and ISO/IEC 27002), which ensures consistency in the implementation of strategic objectives in the context of cybersecurity;

- at the political level – coherence between regulatory requirements, strategic guidelines and/or allied coordination mechanisms (NIS2, NATO CCDCOE, ENISA) is ensured, which is key to the integration of cybersecurity within the framework of national/coalition security.

Along with the advantages of the proposed multidimensional model, it is important to take into account its limitations. They are related to both the degree of maturity and adaptability of the organization, as well as the quality of input and output data for each of the levels. Additional challenges may arise in heterogeneous systems, environments processing classified information, the delay in vertical exchange or the quality of human resources operating at different levels, requiring specific training, experience and knowledge. In this sense, the proposed model should be considered not as a universal solution, but as an adaptive framework, the effectiveness of which depends on the specific application environment and the level of organizational and technological readiness.

The interaction between the tactical, operational, strategic and political levels in the context of cybersecurity is realized through a continuous cycle, in which technical data is transformed into strategic knowledge and management decisions, and these decisions are returned in the form of policies, procedures and technical mechanisms for protection. The lack of an effective connection between these flows leads to gaps, which are prerequisites for the isolated functioning of the detection, response and risk management processes. This necessitates the development of targeted training programs that prepare personnel for positions at relevant levels, provide an understanding of the interrelationships between them and the role of cybersecurity within the framework of national security.

In addition, the horizontal connections in the model complement the vertical integration by ensuring compatibility between different standards and frameworks at the same level. In this way, a comprehensive and interoperable environment is created in which individual standards and frameworks function as mutually complementary elements of a single cybersecurity management system.

VII. EXTENSION OF THE MODEL TO THE SECURITY AND DEFENSE SECTOR

The "Security and Defence" sector is directly related to national security, the stability of society and the protection of critical infrastructure. The continuous evolution of threats, new technologies and globalization have a direct impact on the need to adapt cybersecurity models. In essence, each sector requires unique measures and solutions to address the challenges, but for the "Security and Defence" sector, the specifics are significant. This

includes working with classified information and in a coalition environment, countering hybrid threats, the need for coordination with institutions at the national and international levels. These specifics require the construction of a model that ensures not only technical efficiency, but also compatibility, sustainability and strategic coordination.

The proposed multidimensional model retains its structure of tactical, operational, strategic and political levels, but in the conditions of the "Security and Defence" sector, these levels acquire a specific meaning. At the tactical level, monitoring, detection and basic response are carried out through SOC and command and control systems, and at the operational level, incident management and coordination between different organizational structures, including CSIRT teams, are carried out. The strategic level deals with issues of planning, prioritization and ensuring the resilience of systems and processes, and the political level defines regulatory requirements, policies and mechanisms for coordination with allied and coalition partners.

In this sense, the mechanism of functioning of the proposed multidimensional model for the "Security and Defence" sector can be presented in a graphic form (Fig. 1), illustrating the vertical and horizontal interconnections between the individual levels. Horizontal interaction ensures compatibility between standards, organizational structures and technological environments, which is critical in the conditions of coalition interaction and work with distributed systems.

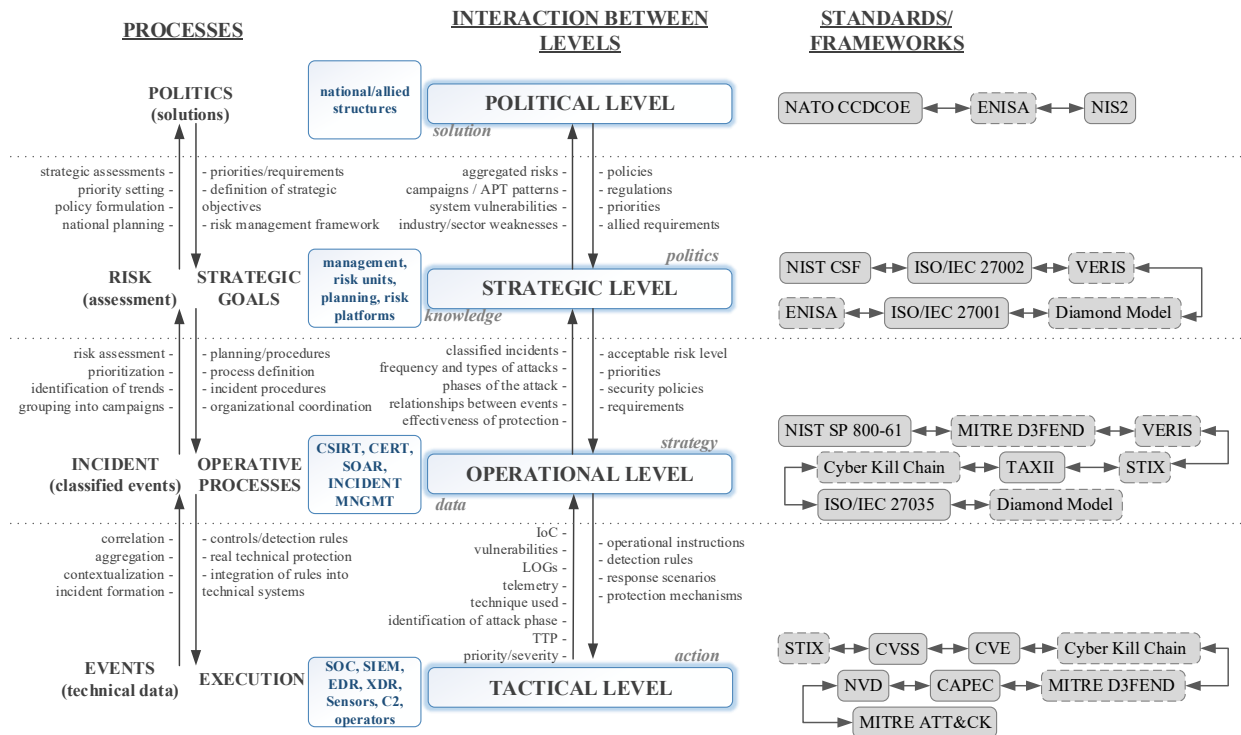


Fig. 1. Multidimensional model for managing cyber incidents in the "Security and Defence" sector.

In the multidimensional model, the flow of information along the vertical is realized as the transformation of technical data (IoC, TTP, vulnerabilities) into incidents, risk assessment, formation of strategic and political decisions, which in turn are transformed back into specific technical protection measures. Frameworks such as MITRE ATT&CK, CAPEC and CVE/NVD/CVSS dominate at the tactical level, while the Cyber Kill Chain and Diamond Model provide an analytical transition to the operational and strategic level. This enables the integration of detection, analysis, management and policies in a single and continuous cycle.

VIII. LIMITED PROOF OF CONCEPT

Illustrative scenario: APT campaign targeting a military information system.

To illustrate the practical application of the proposed multidimensional model, the following scenario describes a simulated APT campaign targeting the information infrastructure of a military information system. The scenario traces the transformation of technical data into strategic and political decisions, and the feedback of those decisions into operational and technical measures, in accordance with the vertical and horizontal interaction mechanisms defined in the model.

Tactical level

Initial indicators of compromise are detected by SOC analysts through SIEM correlation rules and EDR telemetry. Anomalous outbound traffic patterns, lateral movement attempts and credential harvesting activities are identified. Using MITRE ATT&CK, the observed behaviours are mapped to specific techniques (e.g. T1078 – Valid Accounts, T1071 – Application Layer Protocol), while CVE/NVD identifies the exploited vulnerability and CVSS provides a quantitative severity score. CAPEC is applied to characterise the attack pattern, and the Cyber Kill Chain framework is used to determine the phase of the intrusion. All collected indicators of compromise (IoC) and threat intelligence data are structured and formatted using STIX for subsequent exchange and processing.

Vertical Transition (tactical to operational)

The structured technical data — IoC, TTPs, logs and telemetry — is transmitted upward to the operational level, where it undergoes correlation, aggregation and classification as a confirmed incident.

Operational level

The CSIRT, CERT and SOC teams activate the incident management process in accordance with NIST SP 800-61 and ISO/IEC 27035. The incident is classified by type, scope and potential impact. The Cyber Kill Chain and Diamond Model support the analytical transition, providing a structured understanding of the adversary's infrastructure, capabilities and intent. MITRE D3FEND is applied to identify applicable defensive countermeasures, while STIX/TAXII enables the standardised exchange of incident data between national and allied organisational

structures. Organisational coordination is initiated between relevant institutions.

Vertical Transition (operational to strategic)

Classified incident data — including information on the frequency and type of attack, relationships between events and the effectiveness of protective mechanisms — is transmitted to the strategic level for risk assessment and prioritisation.

Strategic level

At the strategic level, the incident is assessed within the frameworks of NIST CSF and ISO/IEC 27001/27002. Risk assessments are conducted, incorporating the CVSS scores generated at the tactical level. Strategic objectives are reviewed, and decisions are made regarding the prioritisation of protective measures, resource allocation and the reinforcement of organisational resilience. VERIS and the Diamond Model support the structured analysis of the incident in terms of its strategic implications. The results of this assessment are consolidated into strategic analyses and recommendations.

Vertical Transition (strategic to political)

Aggregated risk assessments, identified APT campaigns and systemic vulnerabilities are communicated to the political level to inform policy formulation and allied coordination.

Political level

At the political level, NATO CCDCOE, ENISA and NIS2 provide the regulatory and coordination framework. The incident triggers reporting obligations under NIS2 and activates allied coordination mechanisms. Strategic analyses inform the definition of national and coalition cybersecurity policies, regulatory requirements and allied security procedures. Decisions at this level define updated strategic objectives and priorities.

Vertical Feedback (p)

Political decisions and regulatory requirements are translated downward into updated strategic guidelines within NIST CSF and ISO/IEC 27001. These are further operationalised through revised processes and procedures under NIST SP 800-61 and ISO/IEC 27035, and ultimately implemented at the tactical level through updated detection rules, response playbooks and technical protection mechanisms, integrated into SIEM, EDR and XDR platforms using STIX/TAXII-structured data.

This scenario demonstrates that the proposed multidimensional model functions not as a static classification, but as a dynamic and continuous cycle in which technical data, operational decisions, strategic assessments and political actions are mutually interconnected and reinforcing. The horizontal interactions at each level — between standards, organisational structures and technological environments — further ensure the interoperability and coherence necessary for effective cybersecurity governance in the "Security and Defence" sector.

IX. CONCLUSION

The analysis of international cybersecurity standards and frameworks shows that they address a wide range of aspects related to the classification, analysis, management and exchange of information about cyber incidents, but to a certain extent they are also limited because each of them covers only individual elements of cybersecurity (for example: the technical description of vulnerabilities, TTP, IoC, incident or risk management, coordination, interaction, information exchange or other). This confirms the fact that there is no universal framework or standard that can be used independently as a basis for building a comprehensive model, especially in the specifics of cybersecurity and the "Security and Defence" sector.

The proposed multidimensional model, which considers tactical, operational, strategic and political levels and defines the interactions between them vertically and horizontally, ensures a process-based connection of technical data with risk assessment, management decisions and policies. On this basis, and based on the compatibility between different standards and frameworks, organizational structures and technological environments, it is possible to consider cyber incidents not as isolated events, but as part of a broader management and analytical process that can be directly related to national security.

This report does not claim to be an exhaustive review of all existing international standards and frameworks in the field of cybersecurity. The selection of the 19 standards and frameworks was made on the basis of their recognisability, applicability and relevance to the set goal.

The current model has some major limitations that arise from its dependence on the quality of input data at all levels, the degree of organizational and technological maturity, the availability of trained personnel or its use in environments with classified information, especially in the presence of alliance and coalition interaction. For this reason, future research can be directed in several directions. First of all, the inclusion of additional standards, frameworks or models that would expand or complement the current review. Secondly, a detailed examination of the current standards and frameworks and the development of a methodology for validating the model through practical application in a real organizational environment (development of various scenarios, analyses, simulations and exercises). Thirdly, development of modules for training and exercise of various target groups at the tactical, operational, strategic and political levels, so that the model is not only analytical, but also applied educational.

In conclusion, it is important to mention that many standards and frameworks have been developed on a global scale that address various aspects of cybersecurity and in this sense, it is more important not to create new frameworks or standards, but to effectively use, synchronize and integrate existing ones. It is this approach that will allow for reducing fragmentation, achieving clearer connectivity between management levels and creating a unified framework for analysing, managing, prioritizing and dealing with cyber incidents.

ACKNOWLEDGMENT

This scientific report is funded by the Ministry of Education and Science in implementation of the Scientific Program "Security and Defence", adopted by Decree No. 731 of 21.10.2021 and pursuant to Agreement No. D01-74/19.05.2022.

REFERENCES

- [1] The MITRE Corporation, "MITRE ATT&CK", [Online]. Available: <https://attack.mitre.org/>, [Accessed: Nov. 20, 2025].
- [2] The MITRE Corporation, "MITRE D3FEND Knowledge Graph", [Online]. Available: <https://d3fend.mitre.org>, [Accessed: Nov. 20, 2025].
- [3] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, International Organization for Standardization, Geneva, Switzerland, 2022.
- [4] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0", 2024, <https://doi.org/10.6028/NIST.CSWP.29>.
- [5] The MITRE Corporation, "Common Attack Pattern Enumerations and Classifications", [Online]. Available: <https://capec.mitre.org/>, [Accessed: Nov. 20, 2025].
- [6] The Cyber Kill Chain framework, 2011, [Online]. Available: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>, [Accessed: Nov. 15, 2025].
- [7] The NATO Cooperative Cyber Defence Centre of Excellence, [Online]. Available: <https://ccdcoc.eu/>, [Accessed: Feb. 02, 2026].
- [8] Directive (EU) 2022/2555 (NIS2), [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>, [Accessed: Dec. 27, 2025].
- [9] The European Union Agency for Cybersecurity, [Online]. Available: <https://www.enisa.europa.eu/>, [Accessed: Jan. 05, 2026].
- [10] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, International Organization for Standardization, Geneva, Switzerland, 2022.
- [11] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, 2025, <https://doi.org/10.6028/NIST.SP.800-61r3>.
- [12] I.F.Z. Poetiray, M. Salman, "Information security incident management using ISO 27035 standard", Gema Wiralodra, 2023, <https://doi.org/10.31943/gw.v14i3.487>.
- [13] VERIS, "The Vocabulary for Event Recording and Incident Sharing", [Online]. Available: <https://verisframework.org/>, [Accessed: Feb. 15, 2026].
- [14] S. Caltagirone, A. Pendergast, C. Betz, "Diamond Model of Intrusion Analysis," Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, 2013, [Online]. Available: <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>, [Accessed: Jan. 10, 2026].
- [15] National Institute of Standards and Technology, "National Vulnerability Database", 1999, [Online]. Available: <https://nvd.nist.gov/>, [Accessed: Nov. 15, 2025].
- [16] Forum of Incident Response and Security Teams, [Online]. Available: <https://www.first.org/>, [Accessed: Dec. 16, 2026].
- [17] The MITRE Corporation, [Online]. Available: <https://www.mitre.org/>, [Accessed: Nov. 22, 2025].
- [18] OASIS Committee Specification, STIX v. 2.1, January 2021, [Online]. Available: <https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.pdf>, [Accessed: Mar. 25, 2026].
- [19] OASIS Standard TAXII v2.1, June 2021, [Online]. Available: <https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.pdf>, [Accessed: Mar. 25, 2026].

[20] R. K. Yin, "Case Study Research and Applications", 6th ed., SAGE Publications Inc, 2018, USA, ISBN 9781506336169.

[21] D. J. Landoll, "Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments", 3rd ed., CRC Press, 2021, <https://doi.org/10.1201/9781003090441>.

A Hybrid Probabilistic and FMEA-Based Model for Reliability and Fault Tolerance Assessment of AI-Based Security Systems

Silvia Nikolova

Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
silvia_nikolova73@abv.bg

Tsvetoslav Tsankov

Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
c.cankov@shu.bg

Abstract. This study presents a hybrid approach that integrates probabilistic modeling and Failure Mode and Effects Analysis (FMEA) for the analysis and optimization of reliability and fault tolerance in AI-driven integrated security systems. With the increasing complexity of modern intelligent systems—incorporating video analytics, Internet of Digital Things (IoDT) sensors, autonomous drones, and distributed computing infrastructures—there is a growing need for comprehensive methods to evaluate system risk and resilience. A mathematical model based on stochastic processes and Markov chains is developed, enabling quantitative evaluation of failure probabilities and transitions between key system states, including normal operation, degraded mode, and complete failure. In parallel, an FMEA analysis is applied to identify critical components, assess the consequences of potential failures, and calculate Risk Priority Numbers (RPN). The proposed hybrid model integrates probabilistic assessments with expert-driven engineering analysis, resulting in improved accuracy in reliability evaluation. A system-level analysis is conducted across the main subsystems, including the sensing layer, AI processing modules, communication infrastructure, and robotic response units. The results indicate that the communication network and AI modules represent the most critical elements in terms of failure risk. The proposed methodology can be applied in the design, optimization, and management of intelligent security systems, contributing to enhanced robustness, reliability, and operational efficiency under real-world conditions.

Keywords: Artificial intelligence, Fault tolerance, FMEA analysis, Intelligent security systems.

I. INTRODUCTION

A. Relevance of the problem

Modern security systems are undergoing a significant transformation driven by the development of artificial intelligence (AI), the Internet of Things (IoT/IoDT) and

autonomous robotic platforms. Integrated security systems now include multiple interconnected components – video surveillance with intelligent analytics, distributed sensor networks, unmanned aerial vehicles and cloud infrastructures [1]–[4].

This complexity leads to increased requirements for the reliability, availability and fault tolerance of systems, especially when protecting critical infrastructure, industrial sites and urban environments. Failure of an individual component can lead to a significant reduction in efficiency or to a complete failure of the system [5]–[7].

B. Scientific problem

Traditional reliability analysis methods based on classical probabilistic models are often not sufficient for the assessment of complex intelligent systems. On the other hand, methods such as FMEA provide qualitative and expert assessment, but do not include the dynamic behavior of the system over time [8]–[11].

An integrated approach that combines quantitative probabilistic assessment, engineering expert risk assessment and dynamic system behavior is lacking.

This problem is central to modern reliability theory for critical infrastructures, autonomous systems and IoT. Traditional methods (FTA, RBD) often suffer from a lack of failure data for new technologies, while FMEA is a “static snapshot” of risk, not a description of the process over time.

Existing reliability assessment methods such as Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD), and classical probabilistic approaches provide effective mathematical evaluation of hardware reliability but often fail to represent adaptive AI behavior and algorithmic uncertainty. At the same time, traditional FMEA approaches support engineering risk assessment but remain

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.136>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

predominantly static and qualitative. Modern intelligent security systems introduce additional challenges related to false classifications, model drift, adversarial inputs, distributed decision-making, and communication dependency, which are insufficiently addressed in conventional reliability methodologies [12]–[15].

The proposed hybrid approach attempts to bridge this gap by integrating probabilistic state modeling with expert-oriented FMEA analysis, enabling simultaneous evaluation of stochastic system dynamics and engineering risk prioritization.

In order to integrate quantitative probabilistic assessment, engineering expert assessment (qualitative risk) and dynamic behavior, it is necessary to combine several methods in a hybrid framework.

C. Purpose of the study: Failure Modes and Effects Analysis (FMEA)

The main objective of this study is to develop a hybrid model that combines Probabilistic Modeling and Failure Modes and Effects Analysis (FMEA) for reliability assessment, fault tolerance analysis, and architecture optimization of intelligent security systems. This hybrid approach overcomes the limitations of traditional qualitative FMEA by introducing quantitative risk assessment.

D. Research objectives

To achieve the goal, the following tasks are formulated:

- Development of a mathematical probabilistic model
- Modeling of states through Markov processes
- Conducting an FMEA analysis
- Identification of critical components
- Integration of different approaches
- Analysis and optimization of the system

E. Scientific contribution

This research contributes to the field of reliability of intelligent systems by developing an integrated hybrid model combining probabilistic analysis and FMEA. This is achieved by adapting classical methods to AI-based systems and introducing an algorithmic risk assessment approach. The result is the identification of critical components in integrated security systems and the creation of a methodology for optimizing the fault tolerance of intelligent systems [16]–[18].

II. MATERIALS AND METHODS

A. Architecture of the studied system

The considered intelligent security system TEDI (Technological, Electronic, Digital Intelligence) represents an integrated multi-layered structure that includes a variety of interconnected elements (Fig. 1):

- Sensor layer – video cameras, IoT, sensors (motion, temperature, vibration)
- Processing layer – Edge AI (local processing), Cloud AI (centralized processing)

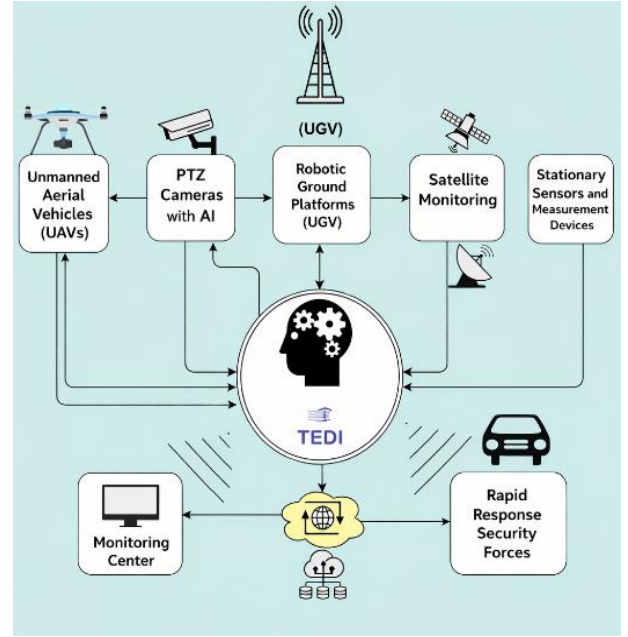


Fig. 1. Architecture of TEDI.

- Communication infrastructure – optical network, wireless communication (5G/LTE), backup channels
- Response layer – autonomous drones, robotic systems, alarm mechanisms

The considered intelligent security system is modeled as a complex stochastic system composed of multiple interconnected subsystems:

$$S = \{S_1, S_2, \dots, S_n\} \quad (1)$$

where each subsystem S_i is characterized by:

- failure rate λ_i
- recovery rate μ_i
- reliability function $R_i(t)$

The system is considered as a combined serial-parallel structure, reflecting the real architecture of intelligent systems [19]–[21].

B. Probabilistic reliability model

Time-to-failure modeling

The time to failure of components is assumed to follow an exponential distribution:

$$R_i(t) = e^{-\lambda_i t} \quad (2)$$

where:

λ_i – failure intensity

System reliability

For a combined structure:

$$R_{\text{system}} = R_{\text{sensor}} * R_{\text{AI}} * R_{\text{comm}} * R_{\text{response}} \quad (3)$$

Parallel structure:

$$R = 1 - (1 - R_1)(1 - R_2) \quad (4)$$

Sequential structure:

$$R = \prod R_i \quad (5)$$

Markov model

The system is modeled using three states:

- S_0 – normal state
- S_1 – degraded state
- S_2 – complete failure

The degraded state S_1 represents partial operational capability caused by subsystem degradation, including communication instability, reduced AI inference accuracy, sensor malfunction, or temporary drone unavailability. The failed state S_2 corresponds to critical operational interruption resulting from simultaneous subsystem failures or unsuccessful recovery processes. Transition probabilities between the states are influenced by redundancy mechanisms, backup communication channels, and recovery procedures integrated within the intelligent security architecture.

Transition matrix:

$$Q = \begin{pmatrix} -\lambda & \lambda & 0 \\ \mu & -(\lambda_r + \mu) & \lambda_r \\ 0 & 0 & 0 \end{pmatrix} \quad (6)$$

The probabilistic behavior is described by:

$$\frac{dP(t)}{dt} = P(t)Q \quad (7)$$

Where:

- λ – failure rate
- λ_r – backup failure rate
- μ – recovery rate

The recovery transition μ reflects the ability of the system to restore operational functionality through redundancy, fault-tolerant architecture, and automated recovery mechanisms.

C. FMEA analysis

Failure Identification

The following subsystems were analyzed:

- cameras
- AI modules
- communication
- drones
- database

Risk Assessment

Each failure is assessed by:

- Severity (S)
- Occurrence (O)

- Detection (D)

Risk index calculation RPN

$$RPN = S \cdot O \cdot D \quad (8)$$

D. Integrated hybrid model

The proposed model combines a probabilistic and FMEA approach:

$$P_{failure} \leftrightarrow RPN \quad (9)$$

Through:

$$Risk_{total} = \alpha P_{failure} + \beta \frac{RPN}{RPN_{max}} \quad (10)$$

where:

RPN – The traditional risk priority number

$Risk_{total}$ – The final, summarized risk assessment for a specific failure mode.

α – Weighting factor for the probability of failure.

β – Weighting factor for the RPN result.

$\alpha, \beta \in [0,1], \alpha + \beta = 1$

$P_{failure}$ – Probability of failure occurrence.

RPN_{max} – The maximum possible value of RPN.

In the present study, the weighting coefficients are selected as $\alpha = 0.6$ and $\beta = 0.4$ in order to provide a stronger influence of probabilistic reliability assessment while preserving the engineering significance of the FMEA evaluation. The selected balance allows simultaneous consideration of stochastic system behavior and expert-based risk prioritization. Higher α values increase the influence of probabilistic failure behavior, while higher β values emphasize engineering risk evaluation through the RPN methodology.

E. Summary of the methodology

The proposed methodology can be reproduced using the presented probabilistic equations, Markov transition structure, and FMEA evaluation procedure. The numerical experiment represents a demonstrative engineering scenario intended to illustrate the applicability of the hybrid model in intelligent security architectures. The sequence of analysis includes subsystem reliability estimation, stochastic state transition modeling, FMEA-based risk evaluation, normalization of results, and integrated hybrid risk assessment.

III. RESULTS AND DISCUSSION

A. Numerical experiment setup

To evaluate the proposed model, an integrated security system with the following subsystems is considered (Table 1):

TABLE 1 SUBSYSTEM RELIABILITY PARAMETERS

Subsystem	Label	Failure Rate λ [1/h]	Repair Rate μ [1/h]
Cameras	S ₁	0.002	0.05
IoT Sensors	S ₂	0.0015	0.04
AI Module	S ₃	0.003	0.06
Communication Network	S ₄	0.004	0.05
Drones	S ₅	0.0025	0.045

Calculation of the reliability of individual components for $t=100$ hours:

$$R_i(t) = e^{-\lambda_i t} \quad (11)$$

Calculation of the reliability of cameras:

$$R_1 = e^{-0.002 \cdot 100} = e^{-0.002} \approx 0.8187 \quad (12)$$

The failure and repair rates used in the numerical experiment are based on representative values from reliability engineering literature, intelligent surveillance systems, industrial communication infrastructures, and expert engineering assumptions. Due to the limited availability of publicly accessible operational datasets for integrated AI-based security systems, several parameters are selected as illustrative values intended to demonstrate the applicability and behavior of the proposed hybrid reliability model.

The communication subsystem is assigned a relatively higher failure rate due to its critical role in distributed data exchange and dependency on network availability. The AI module incorporates both hardware-related and algorithmic reliability factors, while the drone subsystem reflects combined navigation, battery, and communication risks [22]–[24].

$$R_2 = e^{-0.15} \approx 0.8607 \quad (13)$$

Calculation of the reliability of AI:

$$R_3 = e^{-0.03} \approx 0.7408 \quad (14)$$

Calculation of communication reliability:

$$R_4 = e^{-0.04} \approx 0.6703 \quad (15)$$

Calculation of drone reliability:

$$R_5 = e^{-0.25} \approx 0.7788 \quad (16)$$

As a result, the overall reliability of the system with a sequential structure is:

$$R_{system} = R_1 \cdot R_2 \cdot R_3 \cdot R_4 \cdot R_5 \quad (17)$$

$$R_{system} \approx 0.8187 \cdot 0.8607 \cdot 0.7408 \cdot 0.6703 \cdot 0.7788 \approx 0.272 \quad (18)$$

with probability of failure:

$$P_{failure} = 1 - 0.272 = 0.728 \quad (19)$$

The overall reliability with parallel redundancy of the communication with these results is:

$$R_{comm} = 1 - (1 - R_4)^2 \quad (20)$$

$$R_{comm} = 1 - (1 - 0.67)^2 = 1 - (0.32)^2 \approx 0.891 \quad (21)$$

From which a new system reliability is obtained:

$$R_{system,new} = R_1 \cdot R_2 \cdot R_3 \cdot R_{comm} \cdot R_5 \quad (22)$$

$$R_{system,new} \approx 0.8187 \cdot 0.8607 \cdot 0.7408 \cdot 0.8913 \cdot 0.7788 \approx 0.361 \quad (23)$$

The improvement of the system can be calculated by the formula:

$$\Delta R = 0.361 - 0.272 = 0.089 \quad (24)$$

This results in a $\approx 33\%$ relative improvement in system reliability.

For the Markov numerical analysis, the following values are used:

$$\begin{aligned} \lambda &= 0.003 \\ \lambda_r &= 0.002 \\ \mu &= 0.05 \end{aligned}$$

thus, the probability of failure is calculated as follows:

$$\pi_2 = \frac{\lambda \lambda_r}{\mu \lambda_r + \mu \lambda + \lambda \lambda_r} \approx 0.0234 \quad (25)$$

The probability of complete failure $\approx 2.34\%$ in the presence of recovery, which is a significant improvement over the static model.

FMEA numerical analysis (Table 2)

Normalization of results

$$RPN_{max} = 180 \quad (26)$$

$$RPN_{norm}^{AI} = \frac{162}{180} = 0.9 \quad (27)$$

Risk calculation in a hybrid model – Integrated risk in $\alpha = 0.6, \beta = 0.4$:

$$Risk = 0.6 \cdot 0.728 + 0.4 \cdot 0.9 = 0.7968 \quad (28)$$

After optimization

TABLE 2 FMEA ANALYSIS OF THE SYSTEM

No.	Subsystem	Failure Mode	Cause	Effect	S	O	D	RPN	Recommended Action
1	Cameras	Video signal loss	Hardware failure	Loss of monitoring	8	4	3	96	Redundant cameras
2	Cameras	Dirty lens	Environmental conditions	Reduced image quality	5	6	5	150	Auto-cleaning system
3	IoDT Sensors	Invalid data	Calibration error	False alarms	6	4	6	144	Periodic calibration
4	AI Analysis	Misclassification	Poor training	Missed incident	9	3	6	162	Model retraining
5	AI Analysis	False positive detection	Model overfitting	Unnecessary alarm activation	6	4	5	120	Model optimization
6	AI Analysis	False negative detection	Poor training dataset	Missed security incident	9	3	6	162	Dataset retraining
7	AI Analysis	Model drift	Environmental changes	Reduced detection accuracy	8	4	5	160	Continuous learning
8	AI Analysis	Adversarial input	Manipulated visual data	Incorrect classification	9	2	7	126	Adversarial defense mechanisms
9	AI Server	GPU failure	Hardware fault	Processing interruption	8	3	4	96	Backup server
10	Communication Network	Connection loss	Network failure	Data interruption	9	4	5	180	Redundant channels
11	Drone 1	GPS loss	Electromagnetic interference	Navigation failure	7	3	5	105	Inertial navigation
12	Drone 2	Battery depletion	Poor management	Mission interruption	6	5	4	120	Battery monitoring
13	Control Center	Server crash	Software issue	Loss of control	9	2	3	54	Cluster architecture
14	Database	Data loss	Disk failure	Loss of records	8	3	4	96	RAID & backup

$$P_{failure,new} = 1 - 0.361 = 0.639 \quad (29)$$

$$Risk_{new} = 0.6 \cdot 0.639 + 0.4 \cdot 0.6 = 0.6234 \quad (30)$$

Final result (Table 3)

B. Main conclusions from the numerical analysis

Probabilistic model results

The developed probabilistic model allows for a quantitative assessment of the system's reliability over time. When applying an exponential distribution to the individual components, it is found that the overall reliability of the system decreases exponentially, with the rate of degradation depending on the total failure intensity.

For the integrated system we obtain:

$$R_i(t) = e^{-\lambda_{eq}t} \quad (31)$$

where:

$$\lambda_{eq} = \sum \lambda_i \quad (32)$$

TABLE 3 SYSTEM PERFORMANCE BEFORE AND AFTER OPTIMIZATION

Metric	Before	After
Reliability	0.272	0.361
Failure Probability	0.728	0.639
Total Risk	0.797	0.623

The analysis shows that:

- without redundancy, the system is highly sensitive to a single component failure
- with parallel redundancy, a significant increase in reliability is observed
- implementing Edge AI reduces dependence on the central server

Results of the Markov model

The solution of the Markov model shows the probability distribution of the states:

- $P_0(t)$ – normal operation
- $P_1(t)$ – degraded state
- $P_2(t)$ – failure

In steady-state mode, it is found that the probability of a degraded mode is significantly higher than that of a complete failure. Increasing the recovery intensity μ leads to a significant decrease in P_2 , and redundancy reduces the frequency of transition to a failure state.

Results of the FMEA analysis

The FMEA analysis conducted identifies the critical components of the system through the values of the RPN index.

Highest values: Communication network – RPN = 180

Average values: IoDT sensors – 144

Low values: Control center – 54

Graphical analysis of the hybrid model (Fig. 2)

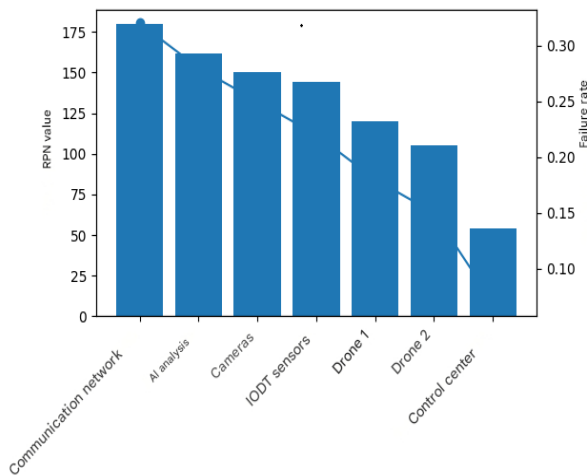


Fig. 2. Risk Priority Number (RPN) Distribution Across System Components.

The graph of RPN values clearly differentiates the criticality of individual components in the system. The highest value is recorded for the communication network (RPN = 180), which defines it as the main source of system risk and a priority for optimization. Components based on artificial intelligence and video surveillance – AI analysis (162) and cameras (150) – also fall into the high-risk zone. This shows that algorithmic errors and the quality of visual data have a significant impact on reliability. IoT sensors (144) and drones (120–105) form a group with medium-high risk, which suggests the need for additional stabilization, but do not represent a critical failure factor. The control center (54) demonstrates the lowest risk, which positions it as the most resilient component in the architecture.

The results obtained show that the reliability of intelligent security systems is highly dependent on the communication infrastructure, the algorithmic stability of AI and the quality of input data. It is particularly important that AI systems add a new type of risk – algorithmic risk, which does not exist in classical systems.

C. Advantages of the proposed model

The hybrid approach offers an integration of quantitative and qualitative methods for a more accurate risk assessment. This allows for prioritization of engineering solutions and is a prerequisite for applicability to complex distributed systems. Despite the undeniable advantages, the model has a number of limitations of the study. These are the use of an exponential distribution (simplification), dependence on expert assessments in FMEA and limited empirical validation. Future validation using real operational datasets and large-scale deployment scenarios may further improve the precision and applicability of the proposed model.

The proposed model can be used in the design of video surveillance systems for the protection of critical infrastructure. The proposed model can also be applied in

the design of Smart City infrastructures and industrial IoT systems.

IV. CONCLUSIONS

This study presents a hybrid approach for the analysis and optimization of the reliability of intelligent security systems, based on a combination of probabilistic modeling and FMEA analysis. The results show that the reliability of the system critically depends on the communication infrastructure, with AI modules being a key factor for fault tolerance. The application of the hybrid approach allows for a more accurate risk assessment.

The proposed model provides an effective tool for the analysis of complex systems and the identification of critical components. The evaluation of the results can be a foundation for architecture optimization.

Future research may include Monte Carlo simulations, as they are a powerful mathematical method for modeling uncertainty and predicting outcomes in complex systems. Also, the analysis can be improved using real operational data. A very important factor for predictive maintenance is machine learning and its extension to cybersecurity and hybrid attacks.

The hybrid probabilistic and FMEA approach represents an effective methodology for analyzing the reliability of modern intelligent security systems, providing a balance between mathematical rigor and engineering applicability [25]–[26].

V. ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to their colleagues from the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen for their valuable support, professional advice, scientific discussions, motivation, and cooperation during the preparation of this research. Their recommendations and constructive feedback contributed significantly to the development and improvement of the present study. This publication is funded by the fund “Support for Publishing Publications in Journals with Impact Factor (IF) and Impact Rank (SJR)” of Konstantin Preslavsky University of Shumen, Republic of Bulgaria.

REFERENCES

- [1] R. Kumar, J. Singh, and Y. K. Dwivedi, “Application of IoT and AI in smart surveillance systems: A systematic review,” *Sustainable Cities and Society*, vol. 70, 102889, 2021.
- [2] X. Xu et al., “Edge–cloud collaborative intelligence for IoT systems,” *Future Generation Computer Systems*, vol. 128, pp. 1–12, 2022.
- [3] C. Alcaraz and J. Lopez, “Cybersecurity in IoT-based smart systems: A review,” *Computer Networks*, vol. 185, 107731, 2021.
- [4] V. Stoyanova, “Analysis of the public communication channels for transmission of hidden information,” in *Proc. Int. Conf. Advanced Research and Technology for Defence (ARTDef)*, 2021, ISSN 2815-2581.
- [5] Z. Chen, K. Zhang, and H. Li, “Reliability modeling of distributed AI systems in edge-cloud environments,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5678–5690, 2022.

- [6] S. Park and J. Kim, "Fault-tolerant architecture for AI-based surveillance systems using edge computing," *Future Generation Computer Systems*, vol. 144, pp. 12–25, 2023.
- [7] P. Singh and V. Sharma, "Fault tolerance in distributed IoT systems: A survey," *Computer Communications*, vol. 182, pp. 1–15, 2022.
- [8] Y. Zhang, M. Xie, and P. Wang, "Reliability analysis of complex systems using Bayesian networks and AI techniques," *Reliability Engineering & System Safety*, vol. 210, 107530, 2021.
- [9] X. Li, H. Chen, and L. Xu, "A hybrid reliability assessment method combining FMEA and Bayesian networks for intelligent systems," *IEEE Access*, vol. 10, pp. 34567–34580, 2022.
- [10] Y. Liu and X. Zhao, "Hybrid probabilistic models for reliability optimization in smart systems," *IEEE Systems Journal*, vol. 17, no. 2, pp. 3456–3467, 2023.
- [11] Q. Zhou et al., "Integrated FMEA and probabilistic risk analysis for intelligent systems," *Reliability Engineering & System Safety*, vol. 232, 109054, 2023.
- [12] Z. Wang and X. Chen, "Hybrid FMEA and Bayesian network for reliability assessment," *Safety Science*, vol. 139, 105239, 2021.
- [13] A. Gupta and S. Srivastava, "Failure mode and effect analysis in cyber-physical systems: A review," *Microprocessors and Microsystems*, vol. 90, 104450, 2022.
- [14] H. Liu et al., "A novel fuzzy FMEA approach for risk assessment in complex systems," *Applied Soft Computing*, vol. 86, 105899, 2020.
- [15] F. Alqahtani and A. Kumar, "Risk assessment of IoT-based smart systems using FMEA and machine learning," *Sensors*, vol. 23, no. 4, 2156, 2023.
- [16] T. Wang, Y. Zhao, and L. Sun, "A Markov-based reliability evaluation method for intelligent monitoring systems," *Applied Mathematical Modelling*, vol. 89, pp. 1102–1115, 2021.
- [17] B. Sun et al., "Reliability analysis of AI-enabled cyber-physical systems," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5890–5901, 2022.
- [18] L. Zhang, X. Wu, and Y. Zhao, "Deep learning-based reliability modeling for complex systems," *IEEE Transactions on Reliability*, vol. 72, no. 2, pp. 456–468, 2023.
- [19] D. Kim and S. Lee, "Edge AI for real-time surveillance: Reliability and performance analysis," *IEEE Access*, vol. 11, pp. 22345–22360, 2023.
- [20] M. Hassan and S. Ali, "Integrated risk management in smart security systems using hybrid models," *Safety Science*, vol. 147, 105621, 2022.
- [21] T. Nguyen and B. Tran, "Reliability and availability analysis of cloud-based AI services," *Journal of Cloud Computing*, vol. 10, no. 1, 45, 2021.
- [22] M. Rahman, S. Islam, and M. Rahman, "AI-driven predictive maintenance for industrial IoT systems," *Computers in Industry*, vol. 137, 103594, 2022.
- [23] J. Torres and L. Martinez, "Reliability engineering in autonomous robotic systems: Challenges and solutions," *Robotics and Autonomous Systems*, vol. 142, 103789, 2021.
- [24] F. Rossi et al., "Reliability challenges in autonomous robotic systems," *Robotics and Autonomous Systems*, vol. 171, 104593, 2024.
- [25] S. Kuutti et al., "A survey of deep learning applications to autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 2, pp. 712–733, 2021.
- [26] E. Zio, "The future of reliability engineering in the era of artificial intelligence," *Reliability Engineering & System Safety*, vol. 215, 107849, 2021.

The Key Role of SMEs in the European Defense Ecosystem with Emphasis on Quantum Technologies

Monika Panayotova

International Relations Department

University of National and World Economy

Sofia, Bulgaria

monika.panayotova@unwe.bg

Abstract— The research paper focuses on the important role of Small and Medium Sized Enterprises (SMEs) in the development of the European defense ecosystem with emphasis on quantum technologies, incl. with dual use. The research is based on interdisciplinary approach. In addition to the methods of analysis and synthesis of primary and secondary sources of information, generalization, inductive and deductive research approach, the study uses Drexler/Sibbet Team performance model as well as Joseph Schumpeter's theory from the entrepreneurial ecosystem, which claims that SMEs play a crucial role in economic development through "creative destruction" and innovation. The research is based on the key strategic documents of the European union such as the White paper for European defense - Readiness 2030, the Quantum Europe Strategy, the Enrico Letta's Report on the Future of the Single Market, the Mario Draghi's report on EU competitiveness, the Sauli Niinistö's Report on Strengthening Europe's Civilian and Military Preparedness and Readiness as well as the Global risks report of the World Economic Forum. The results of the study identify quantum technologies both as innovation drivers, but also as risk multipliers across many domains - security, defense, cognitive warfare and geopolitics. At the same time contrary to the perception that the defense sector is mainly reserved for traditional defense contractors and large established firms, the study shows that SMEs act as key accelerators of dual-use technological innovation and development of market niches due to their agility, flexibility, cross-sector adaptability, and closer ties to civilian markets, making them an important player in the process of building open strategic autonomy for the EU. In conclusion, the publication draws certain conclusions and recommendations for the importance of social dialogue and SMEs' integration into EU defense-industrial ecosystem through their participation in quantum technologies, as it is essential for European defense market and competitiveness.

Keywords— cognitive warfare, competitiveness, EU defence, quantum technologies, SMEs

I. INTRODUCTION

The aim of this publication is to emphasize the role of the small and medium sized enterprises (SMEs) for the development of the defense and quantum industries and to foster awareness of the importance of quantum technologies - not only for science, but also for building resilience, defense and competitiveness in European union (EU).

The article focuses on the nexus between defense, cognitive warfare, innovative quantum technologies, and SMEs, start-ups, scale-ups. The study examines the complex character of the threats and challenges in the contemporary geopolitical, geo-economic, and defense environment, which calls for a paradigm shift toward more effective cooperation at the national and EU levels as well as the active involvement of stakeholders from the European defense and quantum ecosystems in building open strategic autonomy. A special emphasis is placed also on the role of the social dialogue for ensuring trust and legitimacy.

The publication guides readers through the maze of the newly developed strategic documents at the European level in the field of quantum, security and defense, by emphasizing on the importance of SMEs as agent of "creative destruction" and innovation.

The relevance of the study is determined by second quantum revolution which is underway and the changes in the security environment related to the emerging technological threats, the new cognitive battlefield as well as to the lessons learnt from the short case study of Russia-Ukraine war from 2022. It is in line with the: White paper for European defense - Readiness 2030, the Quantum Europe Strategy, the Enrico Letta's Report on the Future of the Single Market, the Mario Draghi's report on EU competitiveness, the Sauli Niinistö's Report on Strengthening Europe's Civilian and Military Preparedness and Readiness as well as the Global risks report of the World Economic Forum.

The publication is particularly timely in light of the forthcoming debate on the Multiannual Financial Framework (MFF) 2028 - 2034 and the proposed new Competitive fund with a total envelope of € 409 billion, as well as the upcoming proposal for legislative Quantum act. The next European budget is expected to be centered on priorities like security and defense, economic competitiveness, and Europe's strategic autonomy, with a central theme of greater agility and flexibility, while the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.186>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

EU Quantum Act will aim to position Europe as a global leader in quantum innovation, ensuring strategic autonomy in this pivotal field.

The research paper consists of the following three points of analysis: 1) European defense and quantum ecosystems with emphasis on SMEs, and through the prism of Joseph Schumpeter's "creative destruction" theory; 2) Quantum Europe Strategy through the lens of Drexler/Sibbet Team performance model; 3) Quantum technologies as innovation drivers and risk multipliers.

II. MATERIALS AND METHODS

The study has been based on institutional analysis and a wide range of official materials, including legal and strategic documents at European, international and national levels dully referenced in the paper.

For the purposes of the publication have been utilized various analytical and synthetic methods, including the analysis and synthesis of primary and secondary sources of information, as well as the methods of induction and deduction, secondary data analysis. The research employs also short case studies from representative European quantum companies and the Ukraine's defense industrial base in order to analyze the changes in modern warfare and the role of SMEs and start-ups in dual-use and quantum technologies.

In addition, an interdisciplinary approach has been implemented, combining political science analysis of the EU, with theories and concepts from the entrepreneurial ecosystem such as - Joseph Schumpeter's theory, which claims that SMEs play a crucial role in economic development through "creative destruction" and innovation as well as the Drexler/Sibbet Team performance model which supports teams in developing and realizing their full potential by outlining seven different stages, each characterized by specific actions and resolved challenges. Moreover, a SWOT analysis was conducted to assess the main strengths, weaknesses, opportunities and threats of the EU quantum's state of play.

III. RESULTS AND DISCUSSION

1) European defense and quantum ecosystems with emphasis on SMEs, and through the prism of Joseph Schumpeter's "creative destruction" theory

Creative destruction plays a key role in entrepreneurship and economic development. Coined by economist Joseph Schumpeter in XX century, the theory of "creative destruction" suggests that business cycles operate under long waves of innovation [1]. The process of creative destruction incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one [2].

SMEs are not only a large part of the economy but also, almost by definition, are at the heart of the Schumpeterian process of creative destruction, since most new firms entering are small (as are most of the exiting firms). The heart of the growth potential of a Schumpeterian business fabric lies in the presumption that small entrants bring to the market new and better processes or products, displacing firms with older and/or less efficient products or technologies. Innovation is at the core of the Schumpeterian growth process and small and medium enterprises are the most promising actors in the Schumpeterian dynamics, as they are considered to have a key role in creating new ideas and developing them into successful innovations. A lack of small new innovators may thus reduce particularly the introduction of radical breakthrough innovations, which lay the foundations of

completely new markets. Missing small new innovators may also reduce the innovativeness of incumbent firms, lacking the challenge to adopt the latest innovations to escape competition and lacking the opportunity to acquire small firm ideas to further improve on [3].

Europe's 25 million SMEs are the backbone of the EU economy. They employ around 100 million people, account for more than half of Europe's GDP and play a key role in adding value in every sector of the economy. SMEs bring innovative solutions to challenges. In the diverse industrial landscape, the space and defense sectors are key for the EU's strategic and technological sovereignty and offer great potential for European SMEs [4].

However, defense and high technological spheres are still very closed and often restricted to established players with proven track records. For the traditional defense industry, it remains difficult to realize that the level of demand is extremely high, funding is insufficient, and the willingness of the public and private sectors to take risks is volatile. In such a situation, the involvement of new players such as SMEs, start-ups and scale-ups does not lead to mutual competition, rather than to mutual complementarity and competitiveness. There is a need of a paradigm shift and it's not about choosing between traditional defense industry companies (which have specific expertise, scale and rich experience) and the new small entrants, but about making them work together to innovate disruptively, balance and compensate speed, cost, and risk. SMEs act as key catalysts for dual-use technological innovation and the development of market niches thanks to their flexibility, ability to adapt across different sectors, and closer ties to civilian markets, making them a key factor in the process of building (open) strategic autonomy for the EU.

The EU's open strategic autonomy refers to its ability to act autonomously (i.e. without depending on other countries) in strategically important policy areas, linked to both the economic and non-economic spheres. These areas may include defense, research, energy, health, media, technology, industry, as well as development cooperation, promotion of democracy, protection and promotion of human rights [5].

In this regard, the European Commission boosts cross-border cooperation and new entrants by maximizing the European Defense Fund, through SME-focused calls, bonuses and award criteria, and stronger links to the wider defense community. It also supports disruptive technologies, allowing companies to take more risk and to create economies of scale by seeking synergies between civil, space and defense industries in EU programmes [6]. According to Sauli Niinistö's Report on Strengthening Europe's Civilian and Military Preparedness and Readiness, the race to control disruptive technologies will intensify as it adds to the arsenal for power and global influence. Disruptive technologies offer untold possibilities by shifting the economic performance, but also come with new vulnerabilities and security concerns related to the transformed nature of warfare (unmanned air and naval systems with AI, encryption keys etc.). In this regard, defense and dual-use-related considerations should be fully embedded in the EU's work on critical technologies, such as AI and quantum, especially in terms of promoting the EU's advances in this field to reduce dependencies and protect against technology leakage [7].

The Russia-Ukraine war from 2022 is a kind of a case study, showing the considerable changes in modern warfare, particularly regarding the speed of innovation cycles, drone proliferation, and electronic warfare evolution. The Center for Strategic and International Studies (CSIS) made a thorough report on how Russian invasion dramatically accelerated transformation of

Ukraine's defense industrial base by focusing on: 1) civilian-military fusion with IT professionals and engineers either joining the armed forces directly or providing technical support as well as 2) decentralized innovation which is beyond formal defense industries, entrepreneurs and small groups emerged as significant innovation sources. Dr. Phillip Karber, professor of military strategy and warfighting at the Eisenhower School observed that major changes in drone technology occur approximately every six months, which is dramatically faster than typical Western defense acquisition timelines. He outlines that: "We in the West, including the United States, are just not keeping up. It takes us six years to get it designed". For software-based weapons systems, Kateryna Bondar, CSIS fellow indicated the innovation cycle could be as short as one to two weeks, with immediate battlefield testing and feedback loops. A critical factor identified as enabling rapid innovation was the direct connection between developers and frontline users. In addition, the president of global government at the American manufacturer of drones "Skydio", Mark Valentine, highlighted how traditional U.S. acquisition processes rely on requirements developed years before contracts are awarded, often based on lessons from previous conflicts rather than emerging threats. He said Skydio's drones, built for U.S. wars in Iraq and Afghanistan with uncontested airspace, struggled in Ukraine's contested electronic environment [8].

Although defense field may seem like the exclusive domain of specific experts and organizations, the complex challenges and the predictable unpredictability suppose a more comprehensive and inclusive approach. The complex character of the threats and challenges in the contemporary geopolitical, geo-economic, security and defense environments require a shift in approach and a change in mindset of the governments and stakeholders for responding adequately and timely. This is not an easy task for sectors that are highly sensitive for countries and their sovereignty, namely defense, security and deep tech industry. Despite the fact that countries recognize that they would struggle to guarantee their security, defense, and competitiveness on their own, their tendency to concentrate resources domestically and share only part of their strategic vision slows the resolution of these challenges and leads to a significant fragmentation of efforts. The situation additionally aggravates, living in the AI and the second quantum revolution era.

The traditional risks reports of World economic forum clearly outline the complex where escalating geopolitical, environmental, societal and technological challenges threaten stability and progress worldwide. They focus on multiple global risks and call for urgent actions to proactively prepare for future shocks. Nowadays, Visa's chief economist, Wayne Best, who refers to "small business as the lifeblood of any economy", even defines the economic risks as "persistent disruptions" rather than "episodic shocks" where success depends on adaptability, resilience and the ability to navigate the constant change [9].

This year 2026 edition reveals again an increasingly fractured global landscape, by emphasizing that the global risks continue to spiral in scale, interconnectivity and velocity. It outlines the following top ten risks in two and ten years' perspectives: 1) in two years outlook (by 2028): Geoeconomic confrontation, Misinformation and disinformation, Societal polarization, Extreme weather events, State-based armed conflict, Cyber insecurity, Inequality, Erosion of human rights and/or of civic freedoms, Pollution, Involuntary migration or displacement; 2) in ten years outlook (by 2036), where environmental and technological risks dominate: Extreme weather events, Biodiversity loss and ecosystem collapse, Critical change to Earth systems, Misinformation and disinformation, Adverse outcomes of frontier technologies (incl. AI and quantum), Natural resource

shortages, Inequality, Cyber insecurity, Societal polarization, Pollution.

According to the report, progress in quantum technologies is likely to accelerate over the next decade as large companies and governments spend more heavily on seeking quantum leadership. Technology convergence between AI/machine learning and quantum computing is accelerating both fields, giving rise to quantum machine learning. As a result, their combined risk landscape is expected to intensify over the next decade, potentially leading to loss of human control [10].

As stated in the White Paper for European Defense - Readiness 2030, the geopolitical rivalries have not only led to a new arms race but have also provoked a global technology race. In this regard, technology is expected to be the main feature of competition in the new geopolitical environment. A handful of critical and foundational technologies like AI, quantum, biotech, robotics, and hypersonic are key inputs for both long term economic growth, and military pre-eminence. Boosting innovation is key. Technology diffusion for commercial use must therefore be reconciled with more rigid technology ecosystems to advance national security objectives. Based on the already identified capability gaps in the member states, the White paper outlines "AI, Quantum, Cyber and Electronic Warfare" as one of the seven key domains which are critical to build a robust European defense. Emphasis is given to defense applications using military AI and quantum computing. As AI, cloud and quantum computing, secure connectivity, autonomous systems and alternative energy reshape fundamentally warfare and transform traditional approaches, the EU declares to launch a European Armament Technological Roadmap, initially focusing on AI and quantum and boosting dual-use investment through EU, national and private funding, including via the European Innovation Council and the planned TechEU Scale-up Fund [11].

As highlighted by Mario Draghi, developing Europe's defense can boost competitiveness and innovation. It also requires a level playing field for public and private enterprises, targeted support for SMEs, resilient supply chains and a more integrated European defense market. The Draghi report on EU competitiveness refers to quantum as "the next trailblazing innovation in the computing field, which could open new opportunities for the EU's industrial competitiveness and technological sovereignty".

According to the former European Central Bank President, Europe needs to develop a strong and independent defense industrial capacity that allows it to meet increasing demand for military assets and equipment and remain at the forefront of defense technology. He highlights that currently the European defense industry is fragmented, limiting its scale and hindering operational effectiveness in the field. It suffers from a lack of standardization and interoperability of equipment, weakening Europe's ability to act as a cohesive power. He emphasizes also that as the EU defense spending rises, defense industrial consolidation, integration and technological innovation should be supported by reinforced European preference principles in procurement, ensuring that a minimum share of this rising demand is concentrated on European companies rather than flowing overseas. Currently, the EU invests around €1 billion in defense R&D per year, but most funding occurs at Member State level, with only one-tenth share at EU level despite overall public R&I spending being comparable to the US as a share of GDP [12].

The Draghi report originally identified three necessities for the EU to boost its competitiveness by: closing the innovation gap; decarbonizing our economy and reducing dependencies. The new European Commission's roadmap for economic growth - "Competitiveness compass" sets out an approach to translate these

necessities into innovation by: 1) creating a friendly environment for young companies to start and expand, with a dedicated EU start-up and scale-up strategy; 2) helping big companies adopt new technologies such as AI and robotics, thanks to the EU Apply AI strategy; 3) making it easier for companies to operate across the EU by simplifying rules and laws, with a proposal for a 28th legal regime to guarantee one set of rules across the EU, including the EU Inc. company form, making it easier to start and grow a business in the EU and attract investments; 4) supporting the development of new technologies, with action plans for quantum, advanced materials, biotech, robotics and space technologies [13].

Defense is a high-tech industry driven by revolutionary innovation, where maintaining strategic advantage demands considerable R&D investment, and quantum technologies offer a dual advantage by enhancing both competitiveness and defense stability. For this reason thinking outside the box alongside with stronger interaction within and between defense and quantum ecosystems are very important as the challenges are growing together with the costs of addressing them. The common denominator for the both ecosystems are the governments, industry, academia, research institutions, SMEs, start-ups and scale-ups. The development of both European defense and quantum markets can further contribute to the suggested by Enrico Letta new dimension of the Single Market, namely the fifth freedom of research, innovation, and education [14] which is expected to catalyze progress in areas such as R&D, data use, AI, quantum computing, biotech, bio robotics, and space.

SMEs have the opportunity to play a more active role both as subcontractors and partners in the value chain and by offering specialized expertise, services and technologies. According to the European Commission data, more than 2500 small and medium-sized enterprises are playing a central role in the complex defense supply chains in Europe. SMEs active in the defense industry are key enablers of innovation and growth, able to conduct essential research, technology and innovation activities. A substantial part of the European Defense Technological and Industrial Base is made of SMEs [15].

Within the defense and quantum sectors and across their points of overlap, it is common that they coexist in a broader ecosystem where some of the companies are coming from other industrial sectors but through the development of dual-use technologies move from civilian to defense and quantum industries.

According to the analysis of the OECD, the quantum industrial ecosystem comprises 4622 organizations, including 830 core companies whose activities are primarily or entirely focused on quantum technologies. Core quantum firms are typically startups that rely heavily on early-stage investment and public funding [16].

This trend of predominance toward SMEs and start-ups continues at EU level where 83% of all full members of the European Quantum Industry Consortium - Europe's largest quantum industry association, are SMEs. As of April 2026, 18 out of 107 companies (16.8%) were large companies, while the remaining are SMEs [17]. The quantum ecosystem is composed of large established and small companies, universities and PROs coming from different other sectors.

The recent mapping of the global quantum ecosystem based on the analysis and data of the European patent office and OECD has revealed that intellectual property, combination of patenting with partnerships, early stage investments and public funding have a key role in the commercialization and industrial scalability of quantum researches. They exemplified it by showing the case studies of two French and one German companies - PASQAL,

C12, and Planqc, that moved beyond theory. Founded in 2019, PASQAL was built on technology transferred from Institut d'Optique through an initial patent, proprietary know-how, trade secrets and the involvement of researchers who later became founders. This approach ensured the effective transfer of intellectual assets and made IP a core foundation of the company. PASQAL develops quantum processors based on neutral atoms, using precisely controlled laser light to trap and manipulate high-performance qubits. The company became a large enterprise with 300 employees and offers both on-premises quantum processing units and cloud-based access through its own platform and providers such as Google Cloud, Microsoft Azure Quantum, OVHcloud and Scaleway. Early validation and adoption were supported by procurement programmes led by the European High Performance Computing Joint Undertaking, which accelerated industrial readiness, market adoption and Europe's strategic quantum computing capabilities.

C12, a Paris-based spin-off from École Normale Supérieure, was founded by twin brothers Matthieu Desjardins and Pierre Desjardins. The company develops quantum computers using carbon nanotubes, a novel approach that promises greater stability and scalability, and launched Callisto, a cloud-based quantum emulator for testing quantum algorithms before physical processors are available. In five years, C12 grew into a 60-person company, raising €30 million and building a strong intellectual property portfolio. C12 emerged from a breakthrough at École Normale Supérieure, where researchers created a highly stable qubit by coupling an electron spin in a carbon nanotube to a microwave photon. The founders partnered with CNRS Innovation to secure an exclusive licence for the foundational patent and adopted a "patent-first, publish-second" strategy, protecting innovations through patents and trade secrets. By 2025, C12 had raised approximately €30 million from investors including 360 Capital, Airbus Ventures, Bpifrance and the European Innovation Council Fund. It established a nanofabrication laboratory in Paris and partnerships with CEA-Leti, OVHcloud, Thales, Air Liquide and TotalEnergies. C12 is another example how a disciplined IP strategy can transform a scientific discovery into a globally competitive quantum technology business platform [16].

Planqc is based in Garching, Germany and has emerged in 2022 from groundbreaking research into one of the leading companies in the development of digital quantum computers. Utilizing this unique technology based on neutral atoms as qubits, Planqc is pursuing the fastest path toward building industry-relevant quantum computers. The company has more than 100 employees from more than 30 nationalities and total funding and contracts secured amounting €80 million [18].

As Schumpeter emphasized the entrepreneurs incessantly create something new which gives them a temporary advantage over their competitors. For this reason, the member states and their established defense industry players need such renewal and "agents of disruptive innovation" that are the first to recognize the signs of the future and turn them into viable businesses [19]. In the economic arena, if you are not open for business, you are out of business. When translated into the language of security and defense policy, this maxim raises the stakes for the very existence of states and the protection of their citizens and territories to a much higher level.

The changes in security environment and the emerging complex threats show the need of rapid innovation and productive civil-military fusion in the European way.

2) *Quantum Europe Strategy through the lens of Drexler/Sibbet Team performance model*

Early national quantum strategies in United Kingdom, European Union, and United States (U.S.) initially focused on research and development, but since around 2021 have increasingly shifted toward commercialization, applications, and industrial deployment, with ongoing policy developments highlighting the need to better translate research into market-ready solutions. According to the OECD analysis - Austria, Czech Republic, Germany, France, Netherlands, Denmark, Finland, Sweden, Spain, Italy and Ireland are working actively on the development in the quantum technologies' field. Some of the countries elaborate comprehensive national quantum strategies and/or formulate relevant policies to support development and adoption of quantum innovations, other rely heavily on EU funding notably NextGenerationEU and its Recovery and Resilience Facility for investing in quantum R&D, infrastructure and collaborative projects, which in turn supported the development or formalization of national quantum strategies [20]. Germany, France, Netherlands are among the most active in the field of quantum technologies and apart from the significant national investments they also initiated a trilateral cooperation with over €30 million for R&D programme.

These countries have a vision with a time horizon 2030 and a strong ambition for sovereignty and leadership in quantum technologies. An interesting moment in the many of already strategic documents and initiatives is each country's ambition to be among the leaders in the field. While this approach can drive progress and outline the champions in Europe, it can also be a drawback as the focus may shift to a competition among member states where the best emerge individually, rather than building a strong, coordinated EU effort capable of competing and winning globally. In this regard, the European commission strives to fill this gap and to secure the EU technological leadership by adopting in 2025 a new strategy on quantum.

Presenting the High Tech Agenda of the German Government at the quantum world congress, Dr. René Haak, Head of Science and Technology, German embassy once said "Quantum is a team sport - and Germany is a team player"[21; 22; 23]. By drawing a similar analogy with the "Quantum Europe Strategy: Quantum Europe in a changing world" and applying the Drexler/Sibbet Team performance model, the analysis attempts to determine at what stage the EU is in its transformation from a group into a team on issues related to quantum technologies. Allan Drexler and David Sibbet are the founders of the so-called Team performance model that illustrates seven key stages for turning a group into a team - orientation; trust building; goal clarification; commitment; implementation; high performance and renewal, dully outlined in Fig. 1. As the member states of the Union are still functioning much more as a group than as a cohesive team on the quantum issues, the model helps for demonstrating the level of its current and potential evolution in the framework of the EU.

The first stage is related to the "orientation". Here the members are supposed to overcome the existing disorientation, fears, uncertainties and to form a common purpose and team identity. Europe's current situation on quantum technologies shows that EU is a global leader in quantum research, concentrating quantum talent and ranking first worldwide in the number of scientific publications in the field of quantum technologies. It is also home to a significant portion of global quantum start-ups. However, Europe lags in commercialization of this technology [25]. In the Quantum Europe strategy, such an "orientation" is given where the EU is currently. On the basis of this analysis and the Quantum Europe strategy, without claiming completeness, the table 1 outlines the main strengths, weaknesses, opportunities and threats of the EU quantum's state of play. The SWOT matrix complements the main text by

synthesizing the main provisions of the strategic document and incorporating additional analytical insights in a concise and structured format.

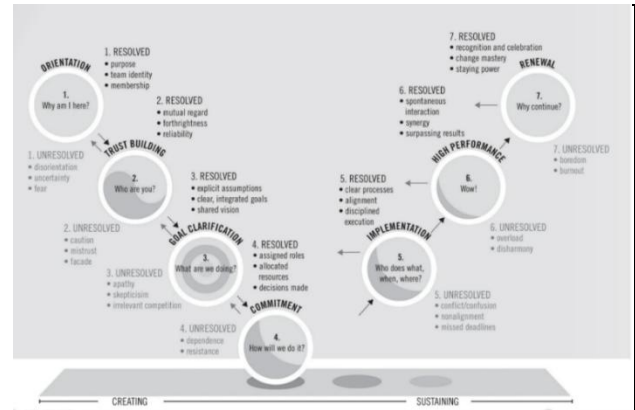


Fig. 1. Drexler/Sibbet Team performance model. The Decision book [24]

TABLE 1: SWOT - QUANTUM EU

<i>Strengths</i>	<i>Weaknesses</i>
-tradition in quantum science research -highly qualified engineers, excellence in research -world's largest concentration of quantum talent -ranks first globally in the number of scientific publications -one of the largest quantum startup ecosystems according to McKinsey & Company (2024) -one third of all quantum companies worldwide are based in the EU	-lagging behind in translating its innovation capabilities and future potential into real market opportunities -Europe's efforts remain fragmented across Member States and funding bodies -duplication of efforts, inefficient use of resources, and growing competition for talent among Member States -undermined EU's ability to build critical mass and scale, slowing down the commercialization pipeline -Europe attracts only 5% of the global private quantum funding, compared to over 50% captured by the USA - five of the top ten tech companies globally in terms of quantum investment are based in the US and four in China -insufficient public and private funding
<i>Opportunities</i>	<i>Threats</i>
-ranks third globally in patents filed for quantum computing, sensing, and communication -uses the full range of opportunities given in the five strategic areas for Quantum Europe - research and innovation, quantum infrastructure, stronger EU quantum ecosystem, dual uses potential quantum technologies (security and defence), quantum skills -simplifies rules and laws, with a proposal for a 28th legal regime to guarantee one set of rules across the EU, especially for innovative SMEs, start-ups and scale-ups	-the loss of EU most promising companies and talent -diminishes the globally competitive EU industrial capacity and increases the gaps in priority areas and market translation -speed of technological development and changes, undermining the democratic oversight and accountability -ecosystem remains fragile, with start-ups facing unstable revenues, limited capital, and low industrial demand. -defense and security instability, threatening the very existence of states and the protection of their citizens, businesses and territories -adverse outcomes of frontier technologies (incl. quantum, AI)

The second stage is related to the "trust building" and better mutual awareness. Here the members are supposed to

demonstrate mutual regard, forthrightness and reliability by overcoming potential caution, mistrust and facade. In the Quantum Europe strategy, EU focuses on strengthening the vibrant and interconnected EU quantum ecosystem through investments in start-ups and scale-ups, securing supply chains and the industrialization of quantum technologies. In addition to the trust among the stakeholders in the ecosystem, a special attention is also given to the public awareness, societal understanding and informed policy engagement in the field of quantum technologies. Moreover, the European economic and social committee (EESC) always stresses on the role of social dialogue and the involvement of civil society for better transparency, legitimacy and accountability of the relevant policies, thus increasing the democratic oversight and public trust. The EESC calls on the Commission to promote public confidence in the new technologies on the one hand, and to identify (at the earliest possible stage) any negative economic, social and employment repercussions on the other [26]. So that, the speed of the technological changes and disruptions should not be at the expenses of the democratic scrutiny.

The third stage is about “goal clarification” and the presence of a shared vision. In the Quantum Europe strategy, EU clearly outlines its level of ambition by 2030 to be an industrial powerhouse and a global market leader in quantum technologies by strengthening its competitiveness, scientific leadership and technological sovereignty.

If every country pushes to be a “leader”, it often leads to fragmentation, duplication of effort, and weaker collective impact. In the geopolitical context and the fast-moving, resource-intensive fields like quantum and AI, that can slow EU down compared to the competitors from Asia and North America. The national ambition in itself is not a challenge as it stimulates countries to be champions and stay in good shape. The European problem lies in the lack of sufficient coordination among these efforts for excellence. For this reason, the EU should think more like a single team competing globally rather than many teams competing internally. In addition, if the team is made up of champions, the chances of success increase significantly.

The fourth stage is about “commitment”. Here the strategic document outlines the five key strategic areas for Quantum Europe - 1) research and innovation by consolidating excellence across Europe to lead in quantum science and its industrial transformation; 2) quantum infrastructures by developing sustainable, scalable, coordinated infrastructure hubs to support production, design, and application development; 3) ecosystem strengthening by securing supply chains and the industrialization of quantum technologies through investments in start-ups and scale-ups; 4) space and dual-use quantum technologies in the field of security and defense by integrating secure, sovereign quantum capabilities into Europe’s space, security and defense strategies, and 5) quantum skills by building a diverse, world-class workforce through coordinated agile education and training systems and programmes and promoting talent mobility across the EU. Specific actions have been identified to meet the strategy’s objectives, such as: launching the quantum Europe research and innovation initiative; establishing a quantum design facility and six quantum chips pilot lines; launching a pilot facility for the European quantum internet; expanding the network of Quantum Competence Clusters across the EU and establishing the European quantum skills academy in 2026, developing a quantum technology roadmap in space with the European Space Agency and contributing to the European armament technological roadmap [27].

While the stages may seem obvious, experience shows that all teams go through each one, and any omitted stage is typically revisited later [24]. The first four stages (Orientation, Trust

building, Goals clarification, Commitment) focus on team formation. The last three (Implementation, High Performance, Renewal) maintain high performance as the team progresses. In the context of quantum technologies, the European union is still forming the team and is at the stage of commitment where members should confirm their specific roles and responsibilities and commit to their part and to the EU team. As defense and quantum security issues remain within the scope of competences of national authorities, here the leaders of the members states represented at the European council together with the relevant competent ministers sitting at the Council of the EU have a key role to play. The Council, as a co-legislator in the process of adoption of the forthcoming Quantum Act will assume legally binding decisions for the member states in three complementarity dimensions: 1) coordination of the relevant research and innovation investments across the Member States, 2) improvement of the EU industrial capacity in designing and producing quantum technologies, 3) ensuring the security and resilience of quantum supply chains [28].

The rest of the stages are related to the - Implementation, High Performance and Renewal. From now on, the EU and its member states are expected to demonstrate clear processes and division of work, alignment and disciplined execution giving the answers of the questions who does what where and when. Having a common vision, pooling and sharing their resources, and acting as a cohesive power that effectively interacts and uses the innovative and technological potential of its ecosystems, would give the Union opportunities for synergy and high performance. Once this is achieved, and even if the results surpass expectations, it is very important to maintain momentum through renewal and change mastery. To this end, the EU should cease developing subsidiary documents alongside the main ones, focus on allocating funds across key areas, promote synergy among member states, traditional defense industry research institutes and SMEs, and provide greater clarity to ecosystem participants on its objectives and how they will be achieved. Using the “creative destruction” and innovation potential of the SMEs, start-ups and scale-ups as well as completing all seven stages of the team performance model, the EU can further develop its open strategic autonomy, being inclusive and open for partnerships and at the same time capable of holding its own in global competition.

3) *Quantum technologies as innovation drivers and risk multipliers*

In the first quantum revolution of the early twentieth century, scientists learned to understand and apply quantum mechanics (the interactions of atoms and particles) enabling technologies like transistors, lasers, and microprocessors that underpin modern systems. Now, a second quantum revolution is underway, as researchers can detect and manipulate individual particles to develop new technologies in computing, sensing, simulation, cryptography, and telecommunications [29].

In the German quantum strategy, quantum technologies are outlined as a future technology that have the potential to disrupt and offer particularly promising prospects for use [22]. According to Australian army research center, a quantum technology is one whose functionality derives from engineering the states of individual quantum systems. This distinguishes quantum technologies from earlier 20th century technologies (for example, lasers, magnetic resonance imaging, semiconductor electronics) that employ quantum phenomena (for example, coherence, quantized energy, tunneling), but do not directly initialize, manipulate and measure the states of individual quantum systems. The qubit (quantum bit) is the simplest quantum system and the basic building block of most quantum technologies, respectively

the number of qubits is the amount of information that can be encoded and processed by the computer [30]. They are already impacting key areas of the economy, giving rise to new solutions to hitherto unsolved problems, new industry players and innovative business models [31].

As stated by OECD, although quantum technologies offer great potential for innovation, they also present considerable risks, especially concerning digital security and privacy. Quantum computers have the capability to compromise commonly used encryption methods, putting financial information, sensitive data and critical infrastructure at risk. Post-quantum cryptography standards have been developed, with adoption and integration into existing systems to follow. In addition, the advanced capabilities of quantum sensors raise concerns about arbitrary or unlawful surveillance and potential privacy infringements. Applications in cryptanalysis, intelligence gathering and weapons development, among others, pose national security risks that are prompting countries to build domestic quantum capabilities [20]. Professor Peter Shor proposed the basis of factoring large numbers into primes using a quantum algorithm that can perform this calculation exponentially faster than a classical computer [32]. Shor's Factoring Algorithm put quantum computing on the proverbial map. By threatening modern cryptography, it forced governments, industries, and the public to take notice of this emerging technology. Decades later, it remains the standard bearer of quantum algorithms. Efforts to protect financial systems and national security continue, as there is a clear geopolitical risk that a state actor could achieve enough quantum power to use Shor's algorithm before quantum-safe cryptography is fully deployed [33].

Quantum technologies have been identified as having substantial disruptive potential across a range of military applications for the future Joint Force. They offer significant military advantage to early adopters especially in the field of communication, navigation, computational power and high precision sensing as well as simulation, encryption and artificial intelligence [30]. Over the past five years, the EU and the Member States have invested more than EUR 11 billion in quantum technologies. While several Member States have developed their own national strategies and roadmaps, insufficient coordination has led to duplication of efforts, inefficient use of resources, and growing competition for talent. In the second half of 2025, the EU has elaborated a comprehensive strategy to secure its leading position for Europe in the global quantum race by supporting the development of these technologies with dual-use potential in the Union [29].

Although strategic documents in many countries, incl., EU ones, often include the three key quantum technologies pillars - computing, sensing and communications, they rarely emphasize in an explicit and exemplified way their application in defense. By contrast, the army of Australia presents them in a clear and accessible way for a wider audience and connects military and civilian quantum research, which is why its information has been used in this publication without claiming to be exhaustive.

a) Quantum computing

The most critical threat lies in quantum computing's ability to break classical cryptography, potentially leading to mass decryption, the collapse of digital trust infrastructures, and cascading impacts across cyber, economic, and physical systems. At the same time, uneven access to quantum capabilities may deepen global inequalities, concentrate economic power, and drive geopolitical competition toward winner-take-all dynamics [10].

As the analysis of the European Parliament research service show, by the 2030s, quantum computers might compromise

traditional cryptography, putting digital infrastructure at high risk in the EU and around the world. Quantum computers pose a significant threat to the security of classical cryptography (symmetric and asymmetric, with asymmetric cryptography more affected than symmetric cryptography by the quantum threat) because they would be able to efficiently solve certain mathematical problems that classical computers struggle with. This is due to the fact that quantum computers operate on quantum mechanical principles, which would allow them to perform certain complex calculations much faster than classical computers. Algorithms to break traditional cryptography using quantum computers already exist, with Shor's algorithm being the most notable example. Post-quantum cryptography (which uses classical computer properties) and quantum cryptography (which uses quantum mechanical properties) are the two types of critical technology able to protect digital infrastructure from quantum computer attacks. Robust post-quantum cryptography algorithms have been identified, but swift and efficient implementation is crucial before malicious actors exploit the power of quantum computers. Experts stress the need for quantum preparedness to be put in place now, with some of them even warning of a 'quantum cybersecurity Armageddon'. The EU's security union strategy and cybersecurity strategy both highlight encryption as a key technology for achieving resilience against cyber-attacks (e.g. for securing digital systems and defense capabilities) [34].

The EU plans to develop in 2026 its Quantum Computing and Simulation Roadmap. In addition, it outlines its ambition to expand the number and capacity of EuroHPC-based quantum computing systems and set up a monitoring framework for quantum computing. The long-term goal is of achieving a full-stack quantum computing capability by 2030 [29]. Rather than replacing high-performance computing (HPC) systems, quantum computers are expected to complement them, acting as accelerators to boost the overall performance of the computing solution, delivering results much faster and in a much more energy efficient way.

Breakthroughs in quantum computing could also rapidly accentuate economic and industrial inequalities among countries. Disparities in access to existing technologies have already created a digital divide, which is likely to become deeper with quantum [35].

Examples for potential technologies in the field could be: Noisy Intermediate - Scale Quantum computers (incl. integrated in classical networks), error-corrected mainframe computers (incl. capable of cryptography; in quantum networks). The nearest term and lowest technological risk being in delivering enhanced image/signal processing, planning and autonomous systems. Specifically in the defense can be outlined the following: 1) Enhanced signal and image processing and searching intelligence, surveillance and reconnaissance (ISR). Edge quantum computers can improve filtering, decoding, and feature identification in signals and images from ISR devices, reducing network congestion from raw data streaming. Distributed and centralized quantum computers may also expand the ability to search and extract intelligence from large unstructured databases; 2) Enhanced optimization of plans and logistics. Quantum computers may be employed at various levels to provide timely optimization of complex plans and logistics systems; 3) Enhanced artificial intelligence/machine learning in automation, robotics and cyberwarfare. Quantum computers promise to accelerate machine learning sub-routines, learning, and model optimization, enabling enhanced performance and in-mission relearning. Combined with improved signal and imaging processing, this may enhance decision-making in autonomous systems, robot populations, and new cyber tools; 4) Enhanced operational simulation and geophysical modelling. Quantum computers can

accelerate the simulation of stochastic dynamics and complex differential equations (e.g., weather, ballistics, ocean dynamics), supporting superior decision-making; 5) Enhanced defense science and industry. Quantum computers offer unprecedented capabilities in simulating complex molecules and materials, accelerating innovation in bio-/nano-technology and materials engineering. They can also enhance engineering design and process optimization, enabling higher-performing technologies and more efficient manufacturing; 6) New cryptography capabilities. Quantum computers could break public key encryption using efficient factoring algorithms, though this requires many error-corrected qubits and is unlikely within the next 10 years. However, as this falls within the lifetime of some cryptographic systems, the risk must be considered. New decryption methods may emerge, driving a race between decryption and encryption technologies.

b) Quantum sensing

According to the World Economic forum, quantum sensing is starting to lead to important enhancements in military and industrial applications and the leading players in the field are United States, China and Germany. The risks report outlines the emerging practical applications of quantum sensing for military use such as the quantum sensing's potential to be able to identify submarines or stealth aircraft via gravitational or magnetic anomalies, putting at risk key military assets [10]. These technologies and applications in positioning, navigation and timing, detection of gravitational and magnetic anomalies and microwave spectroscopy are valuable in defense [30].

As outlined in the Quantum Europe Strategy, quantum sensing uses quantum properties to measure physical features with unprecedented sensitivity and precision, significantly surpassing classical sensor capabilities. A special focus has been given to the quantum gravimeters, Quantum Magnetic Resonance Imaging (Q-MRI) and to the forthcoming development of a European Quantum Sensing Roadmap. In 2026 the Union is planning the deployment of a distributed system of gravimeters across Europe - a network of mobile and stationary quantum gravimeters, which allow for the detection of subsurface features located up to several tens of kilometres underground, including water reservoirs, gas deposits, mineral resources, magma chambers, or buried infrastructure. In parallel, the EU is planning to launch a first quantum space gravimetry Pathfinder Flight after 2030 and to develop ground, airborne and space-based gravimeters for Earth observation purposes, supporting both scientific research and strategic applications, including those with dual-use potential [29]. Examples for potential technologies in the defense field could be: 1) Enhanced positioning, navigation and timing. Quantum accelerometers, magnetometers, gyroscopes, and clocks offer the stability and precision needed for accurate GPS-independent navigation. Advanced atomic clocks also enable precise timing, improving positioning and digital communications, and enhancing robotic, autonomous, missile, Command, Control, Communications, Computer (C4I), and fire control systems; 2) Enhanced situational awareness. Quantum gravimeters and magnetometers enable advanced geospatial mapping and anomaly detection, such as locating subterranean structures. Quantum microwave spectrometers offer high sensitivity and continuous detection, enhancing radar range and precision and improving detection of electromagnetic emitters; 3) Enhanced medical and environmental analysis. Quantum nanosensors offer unprecedented capabilities for biological and chemical sensing and imaging in medical diagnosis, treatment, and environmental monitoring. These range from injectable nanoparticles for tracking and imaging to lab-on-a-chip analysers and enhancements to existing techniques like Magnetic Resonance Imaging (MRI); 4) Enhanced human-machine interfacing. Quantum magnetometers may enable wearable high-

resolution magnetoencephalography for real-time brain activity imaging, which could be a key step toward practical non-invasive cognitive communication with machines; 5) Enhanced defense science and industry. Quantum microscopes, spectrometers, and nanosensors can drive innovation in materials science and nano-, bio-, and medical technology. They enable advances such as imaging complex molecules for drug design and chip-scale Nuclear Magnetic Resonance (NMR) spectrometers that expand access to precision chemical analysis [30].

c) Quantum communication

Quantum communication enables ultra-secure data transmission, protects critical infrastructures, and safeguards sensitive information against future quantum-enabled cyber threats. It also enables to establish quantum communication networks necessary for interconnecting quantum devices such as sensors and computers, into a so-called 'Quantum Internet'[29]. Quantum communications is about the use of quantum networking protocols for the purposes of establishing trusted communications links between sites. Quantum networking allows the transmission of information in the form of qubits between quantum computers, sensors and memory. Quantum networking is expected to allow the development of larger quantum computers from connecting smaller, modular systems of qubits and performing larger distributed computations between them [31]. Quantum communications can be used also to network quantum sensors to correlate and enhance sensitivity over large areas (for example, synchronize clocks within a communication network). Quantum communications can securely access remote quantum computers or transmit data between classical devices (e.g., encryption keys). This is called Quantum Key Distribution (QKD), which enhances security by enabling the safe exchange of one-time private encryption keys between remote nodes of a conventional encrypted network. Security in quantum communications is physically assured by the projective nature of quantum measurements, making it impossible to copy qubit information without modifying it. Interception can thus be detected with known statistical confidence, which depends on the number of qubits used to distill the encryption key and the noise in the communication channel [30].

Thanks to its dual-use potential, it is supporting both civilian applications (e.g., protecting financial transactions, securing public networks) and defense needs (e.g., secure communications for military and national security operations). Through initiatives like the EuroQCI [36] and the Quantum Internet, the EU is building fully autonomous and trusted quantum communication infrastructures, which will protect critical data flows, secure public communications and critical infrastructures, and strengthen Europe's internal security [29]. Applications in the field include: Quantum cryptography including QKD for secure cryptographic key establishment; Quantum radio frequency receivers; Quantum network repeaters for long-distance transfer of quantum-encoded information; Quantum random number generators for improved randomness in cryptography; Transfer of quantum sensor data for storage, computation, or quantum machine learning. Specifically in defense sector can be outlined the following: 1) Enhanced security of communication via QKD. QKD securely distributes one-time private encryption keys, enhancing the security of encrypted communication over public key methods; 2) Enhanced network synchronization. Distributing entanglement can be used to precisely synchronize distant clocks, improving the speed and accuracy of digital communications and enabling better detection and localization of anomalies through correlated sensors; 3) Enhanced sensitivity and large-area quantum sensing. Quantum communications can entangle quantum sensors, improving their combined sensitivity beyond classical limits. Entangling distant sensors also enhances their ability to correlate measurements and more precisely detect or locate anomalies; 4) Enhanced security

and performance of quantum computing. Quantum communications can enhance data exchange between quantum computers, combine their computational power, and enable secure access. Networking them is expected to expand performance and applications, similar to the impact of the internet on classical computers [30].

d) Quantum cognition, technologies and cognitive warfare nexus

Just as the development of new technologies transforms the security and information environment, the new threats arising within that environment likewise influence the ways these technologies are applied.

With the digital transformation of the economies and societies worldwide, an increasingly active new battlefield has seen emerging, which often lies in the so-called “gray zone” between peace and war. This is the cognitive warfare, which was suggested by the NATO Allied Command Transformation (ACT) Innovation Hub to be considered as the sixth operational domain alongside with the land, air, sea, cyberspace, and space. Cognitive warfare can be viewed both as a standalone phenomenon and as part of hybrid warfare, which involves the combination of kinetic and non-kinetic instruments and tactics. The European Union, for its part, views the challenges associated with it within the broader framework of hybrid threats. Retired Lieutenant-Colonel of the French Army François du Cluzel, defines cognitive warfare as the “manipulation of the enemy’s cognition” aimed at weakening, influencing, delaying, and even destroying the enemy [37]. Cognitive warfare influences human decision-making and extends its reach to the public, society, and the military. Information is weaponized across numerous platforms to target individuals, governments, and mass consciousness, justifying adversaries’ strategic objectives. Cognitive Warfare can also be described as the use of all knowledge, strategies, and available tools to impact human behavior through cognition, with the end goal of manipulating and altering decision-making [38].

The nexus between cognitive warfare and quantum cognition, computing and sensing can be viewed as mutually reinforcing. As stated in the Chief Scientist Research Report on Cognitive Warfare: NATO is entering an era of disruptive technologies that affect cognition and human life in both war and peacetime. Here two perspectives can be considered the one of Jerome Busemeyer and Peter Bruza related to quantum models of cognition and decision, and the other one of the Australian army about the most promising quantum technology applications related to enhanced human-machine interfacing (HMI) and magnetoencephalography where engineering meets human psychology by considering consumers’ preferences and instincts. Jerome Busemeyer shows how to use quantum theory to compute probabilities for cognitive and decision-making applications. It is a mathematical theory about the human behavior, focusing primary on judgements and decisions. The quantum models of cognition and decision related to question order effects, conjunction and disjunction errors, compability and quantum rationality, concept combination and human semantic space, conjoint memory recognition and episodic overdistribution effect, bistable perception application and categorization decision-making reveal on how people make context-dependent and non-classical decisions [39]. This is particularly relevant to the cognitive warfare where opponents use uncertainty, ambiguity, emotional conditioning, and the resulting effects to influence decisions. Considering that the “brain is the battlefield of the future” as Dr. James Giordano farsightedly declared several years ago, another important aspect is the use of quantum technologies for data collecting and visualizing in real time the human brain and reactions. Enhanced human-machine interfacing. Quantum magnetometers may enable wearable high-resolution magnetoencephalography for real-time brain activity imaging - a key ingredient to practical non-invasive cognitive

communication with machines. Magnetoencephalography is a non-invasive technique for investigating human brain activity. It’s a neuroimaging technique for mapping brain activity by recording magnetic fields produced by electrical currents occurring naturally in the brain, using very sensitive magnetometers [30].

The competition for citizens’ minds and emotions as voters and consumers are taking an increasingly central role that impact both the democratic societies and markets development. In this regard, quantum cognition and technologies can be both a cause for emergence and a tool for overcoming the vulnerabilities in open and democratic societies.

IV. CONCLUSIONS

On the basis of the analysis provided, the following three key conclusions can be drawn:

1) The SMEs as part of the European defense and quantum ecosystems are of key importance for the development of European defense and competitiveness and for building an open strategic autonomy that gives the EU the opportunity to be simultaneously inclusive and willing for international partnerships and at the same time capable of standing on its own in the global competition. The ongoing second quantum revolution is paving the way for new waves of innovation and the emergence of new technological threats, which require speed, flexibility, cross-sector adaptability and creative destruction potential of the SMEs for recognizing the signs of the future and turn them into viable dual-use businesses.

2) While new technologies are transforming the landscape of security and the information environment, emerging threats are simultaneously shaping their application, which can be viewed in the context of the use of quantum technologies in cognitive warfare. The changes in security environment and the emerging complex threats show the need of rapid innovation and productive civil-military fusion in the European way. The interrelated global risks and the lessons from the war in Ukraine show the need of a paradigm shift in member states and traditional defense contractors and large established firms in order to use the full potential of the EU defense and quantum ecosystems, involving and cooperating with SMEs, start-ups and scale-ups, keeping European scientific and entrepreneurial talents and seeking synergies between civil and defense industries. The global predictable unpredictability supposes a more comprehensive and inclusive approach, a true European spirit and shared vision among the member states, completing all the seven stages for transforming their group into an EU “champion team”.

3) Quantum technologies could be innovation drivers, but at the same time risk multipliers. As outlines the World economic forum “quantum” is set to become a large new industry in itself, creating a new manufacturing supply chain, new quantum service business models (e.g. subscriptions to access quantum computing time) and generating a new set of high-skilled jobs. At the same time the national quantum strategies, namely the one of Australia clearly demonstrates quantum defense applications with special focus on quantum computing, sensing and communication that have the potential to significantly shape the battlefield of the future. In this regard, the investments in defense and advanced technologies’ capabilities must go hand in hand with raising public awareness and improving societal understanding, trust, and informed engagement in quantum and defense policies. In this context, social dialogue and civil society play also a key role in translating policies into citizens’ language, while ensuring that the pace of technological change and transformation does not come at the expense of the democratic oversight.

REFERENCES

- [1] World Economic Forum, "Waves of Change: Understanding the Driving Force of Innovation Cycles," Jul. 5, 2021. [Online]. Available: <https://www.weforum.org/stories/2021/07/this-is-a-visualization-of-the-history-of-innovation-cycles/>. [Accessed: May 3, 2026].
- [2] J. A. Schumpeter, *Capitalism, Socialism, and Democracy*, 3rd ed. New York, NY, USA: Harper & Brothers, 1950, p. 83.
- [3] R. Veugelers, A. Ferrando, S. Lekpek, and C. T. Weiss, *Young SMEs: Driving Innovation in Europe?* Luxembourg: European Investment Bank, Sep. 2018. [Online]. Available: https://www.eib.org/files/efs/economics_working_paper_2018_07_en.pdf. [Accessed: May 3, 2026].
- [4] European Commission, *An SME Strategy for a Sustainable and Digital Europe*, COM(2020) 103 final. Brussels, Belgium: European Commission, Mar. 10, 2020. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0103>. [Accessed: May 3, 2026].
- [5] European Commission, Community Research and Development Information Service (CORDIS), "Open Strategic Autonomy, Economic and Research Security in EU Foreign Policy." [Online]. Available: https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL2-2025-01-DEMOCRACY. [Accessed: May 3, 2026].
- [6] European Commission, *A New Industrial Strategy for Europe*, COM(2020) 102 final. Brussels, Belgium: European Commission, Mar. 10, 2020. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0102>. [Accessed: May 3, 2026].
- [7] S. Niinistö, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness: Report to the European Commission*. Brussels, Belgium: European Commission, Oct. 30, 2024. [Online]. Available: https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinsto-report_Book_VF.pdf. [Accessed: May 3, 2026].
- [8] M. Slusher, K. Auchenbach, S. Murphy, Q. Packard, S. Pence, and L. Slivinski, "Conflict in Focus: Lessons from Russia-Ukraine," Center for Strategic and International Studies (CSIS), Defense and Security Department, May 2, 2025. [Online]. Available: <https://www.csis.org/analysis/conflict-focus-lessons-russia-ukraine>. [Accessed: May 3, 2026].
- [9] World Economic Forum, *Radio Davos*, "We have entered the age of 'persistent disruption' - Visa's Wayne Best on the Chief Economists Outlook," Sep. 23, 2025. [Online]. Available: <https://www.weforum.org/podcasts/radio-davos/episodes/chief-economists-outlook-visa-wayne-best/>. [Accessed: May 3, 2026].
- [10] World Economic Forum, *Global Risks Report 2026*. Davos, Switzerland: World Economic Forum, Jan. 14, 2026. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf. [Accessed: May 3, 2026].
- [11] European Commission, *Joint White Paper for European Defence Readiness 2030*. Brussels, Belgium: European Commission, Mar. 19, 2025. [Online]. Available: https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf. [Accessed: May 3, 2026].
- [12] M. Draghi, *The Future of European Competitiveness: A Competitiveness Strategy for Europe*, Part A. Luxembourg: Publications Office of the European Union, 2025. [Online]. Available: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en. [Accessed: May 3, 2026].
- [13] European Commission, *A Competitiveness Compass for the EU*, COM(2025) 30 final. Brussels, Belgium: European Commission, Jan. 29, 2025. [Online]. Available: https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en?filename=Communication_1.pdf. [Accessed: May 3, 2026].
- [14] E. Letta, *Much More Than a Market: Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens*, Apr. 2024. [Online]. Available: <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>. [Accessed: May 3, 2026].
- [15] European Commission, *The Defence Transfers Directive Handbook for SMEs*. Brussels, Belgium: European Commission, Mar. 8, 2022. [Online]. Available: https://defence-industry-space.ec.europa.eu/document/download/204e50b7-d558-4c52-bfe9-6b578a141c20_en. [Accessed: May 16, 2026].
- [16] Organisation for Economic Co-operation and Development (OECD), *Mapping the Global Quantum Ecosystem: A Comprehensive Analysis Based on Innovation, Firm, Investment, Skills, Trade and Policy Data*. Paris, France: OECD Publishing, Dec. 2025. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/mapping-the-global-quantum-ecosystem_47891dd2/20251217-0001.pdf. [Accessed: May 16, 2026].
- [17] European Quantum Industry Consortium, *Member List (as of 16 April 2026)*. [Online]. Available: <https://www.euroquic.org/wp-content/uploads/2025/05/QuIC-Member-list-16042026.pdf>. [Accessed: May 16, 2026].
- [18] planqc, "From Lab to Impact." [Online]. Available: <https://planqc.eu/>. [Accessed: May 16, 2026].
- [19] Мегатромяна. Светът през 2050. София: Класика и Стил, 2012, pp. 265–266. (*Megapromyana. Svetit prez 2050. Sofia: Klasika i Stil, 2012, pp. 265–266.*)
- [20] Organisation for Economic Co-operation and Development, "An Overview of National Strategies and Policies for Quantum Technologies," *OECD Digital Economy Papers*, no. 379. Paris, France: OECD Publishing, 2025. [Online]. Available: <https://doi.org/10.1787/5e55e7ab-en>. [Accessed: May 3, 2026].
- [21] Federal Ministry of Education and Research (BMBF), *Quantum Technologies: Conceptual Framework Programme*. Bonn, Germany: Federal Ministry of Education and Research, Apr. 2023. [Online]. Available: https://www.bmfr.bund.de/SharedDocs/Downloads/DE/2024/2024-12-11-handlungskonzept-quantentechnologie-en.pdf?__blob=publicationFile&v=2. [Accessed: May 3, 2026].
- [22] Federal Ministry of Education and Research (BMBF), *Developing new technologies: High-Tech Agenda Germany*. [Online]. Available: https://www.bmfr.bund.de/EN/Technology/HightechAgenda/HightechAgenda_node.html. [Accessed: May 3, 2026].
- [23] Quantum World Congress, "Germany Outlines Quantum Strategy Focused on Error-Corrected Systems, Applied Research, and International Collaboration," Nov. 18, 2025. [Online]. Available: <https://www.quantumworldcongress.com/news-and-updates/germany-outlines-quantum-strategy-focused-on-error-corrected-systems-applied-research-and-international-collaboration>. [Accessed: May 3, 2026].
- [24] M. Krogerus and R. Tschäppeler, *The Decision Book: Fifty Models for Strategic Thinking*, rev. ed. New York, NY, USA: W. W. Norton & Company, 2017, pp. 140–143.
- [25] European Commission, "Questions and Answers on the EU Quantum Strategy," Brussels, Belgium, Jul. 2, 2025. Available: https://ec.europa.eu/commission/presscorner/detail/en/qanda_25_1683. [Accessed: May 3, 2026].
- [26] European Economic and Social Committee, *Quantum Strategy*, Opinion INT/1098-EESC-2025, adopted Jan. 21, 2026. [Online]. Available: <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/quantum-strategy>. [Accessed: May 3, 2026].
- [27] European Commission, Directorate-General for Communication, "The EU's Plan to Become a Global Leader in Quantum by 2030," Jul. 2, 2025. [Online]. Available: https://commission.europa.eu/news-and-media/news/eus-plan-become-global-leader-quantum-2030-2025-07-02_en. [Accessed: May 3, 2026].

- [28] European Parliament, "Quantum Act," *Legislative Train Schedule*, Apr. 20, 2026. [Online]. Available: <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-quantum-act>. [Accessed: May 3, 2026].
- [29] European Commission, *Quantum Europe Strategy: Quantum Europe in a Changing World*, COM(2025) 363 final. Brussels, Belgium: European Commission, Jul. 2, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy>. [Accessed: May 3, 2026].
- [30] Australian Army, *Army Quantum Technology Roadmap*. Canberra, ACT, Australia: Commonwealth of Australia, Apr. 2021. [Online]. Available: https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf. [Accessed: May 3, 2026].
- [31] World Economic Forum, *Quantum Economy Blueprint*. Geneva, Switzerland: World Economic Forum, Jan. 16, 2024. [Online]. Available: <https://www.weforum.org/publications/quantum-economy-blueprint/>. [Accessed: May 3, 2026].
- [32] S. Bhattacharyya, "Shor's Algorithm: How Does It Work? Finding Prime Factors of Integer Using Quantum Computer," 2022. [Online]. Available: <https://medium.com/a-bit-of-qubit/shors-algorithm-how-does-it-work-aa6153646419>. [Accessed: May 3, 2026].
- [33] Classiq, "Shor's Algorithm Explained," *Classiq's Library*, Jul. 19, 2022. [Online]. Available: <https://www.classiq.io/insights/shors-algorithm-explained>. [Accessed: May 3, 2026].
- [34] S. De Luca and T. Marcellin, *Quantum Technologies*, PE 766.237. Luxembourg: European Parliamentary Research Service (EPRS), Nov. 2024. [Online]. Available: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI\(2024\)766237_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI(2024)766237_EN.pdf). [Accessed: May 3, 2026].
- [35] J. Hidary and A. Sarkar, "The World Is Heading for a 'Quantum Divide': Here's Why It Matters," *World Economic Forum*, Jan. 18, 2023. [Online]. Available: <https://www.weforum.org/stories/2023/01/the-world-quantum-divide-why-it-mattersdavos2023/>. [Accessed: May 3, 2026].
- [36] European Commission, "European Quantum Communication Infrastructure (EuroQCI)," *Shaping Europe's Digital Future*. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>. [Accessed: May 3, 2026].
- [37] F. Du Cluzel, *Cognitive Warfare: A Battle for the Brain*, STO-MP-AVT-211, STO-MP-HFM-334. Neuilly-sur-Seine, France: NATO Science and Technology Organization, 2021. [Online]. Available: <https://www.sto.nato.int/document/cognitive-warfare/>. [Accessed: May 3, 2026].
- [38] NATO Science and Technology Organization, Office of the Chief Scientist, *NATO Chief Scientist Research Report on Cognitive Warfare*. Brussels, Belgium: NATO Science and Technology Organization, 2025. [Online]. Available: <https://www.sto.nato.int/document/cognitive-warfare/>. [Accessed: May 16, 2026].
- [39] J. R. Busemeyer and P. D. Bruza, *Quantum Models of Cognition and Decision*. Cambridge, U.K.: Cambridge University Press, 2012.

Climate-Induced Migration to the EU: Legal Protection Gaps and the Role of Media Narratives

Vasil Pavlov
University of National and World
Economy
Sofia, Bulgaria
vpavlov@unwe.bg

Raquel Cardoso
Lusiada University/CEJEIA
Porto, Portugal
rcardoso@por.ulusiada.pt

Panagiota (Naya) Kalfeli
Aristotle University
Thessaloniki, Greece
nkalfeli@jour.auth.gr

Abstract— Climate change, along with political persecution, military conflicts, and poor socio-economic conditions, is one of the key drivers of forced migration. This issue has become increasingly relevant, especially in light of rising global temperatures, storms, droughts, sea-level rise, and resource depletion. However, international law currently offers limited protection for climate-displaced persons. This paper has three main objectives: first, to examine the current state of immigration in the European Union (EU) by analyzing official Eurostat secondary data; second, to identify gaps in migration and environmental law; and third, to examine the dominant media narratives surrounding climate-induced migration and the ways in which they shape public understanding and decision-making related to this phenomenon. By doing so, it aims to formulate specific, comprehensive, rights-based recommendations to address the humanitarian and legal challenges of climate-induced migration, while also promoting more accurate, responsible and contextualized media coverage of the phenomenon.

Keywords— Climate Change, Migration, European Union, Legal Framework, Media Narratives

I. INTRODUCTION

Climate change and related natural disasters, such as rising landscape and sea temperatures, intensified storms, and prolonged droughts, represent a key global challenge, as they lead to negative socio-economic effects, among which are a lack of essential resources, poverty, and health risks. These security shortcomings collectively force millions of individuals to flee their countries of origin in search of a better life. This is evidenced by a United Nations (UN) publication that argues that, in 2024, 45.8 million people were displaced due to weather-related disasters [1]. Notably, the publication adds that the majority of displaced populations originate from states that are among the most vulnerable and least equipped to adapt to the adverse effects of climate change. Similar observations are indicated in the Internal Displacement Monitoring Centre's [2] report on Global Internal Displacement, according to which, as of the end of 2023,

7.7 million people had been displaced by disasters worldwide.

Although climate change is often framed as a future concern, its impacts are already palpable and increasingly devastating. The National Oceanic and Atmospheric Administration (NOAA) emphasizes that climate change negatively impacts societies in many different ways – from harming food production and human health, through the widening spread of disease and death, damaging ecosystems and infrastructure, to reducing the overall productivity of the economy [3]. Furthermore, despite clear evidence that climate change affects human mobility, the media and policymakers' narrow focus on defining "climate refugees" oversimplifies the issue and risks overlooking its broader complexity, as stated by the UN International Organization for Migration [4]. Additionally, this source considers that the distinction between "climate migrants" and "climate refugees" is crucial, as the current international legal framework does not explicitly recognize climate migrants as refugees, thereby leaving many without formal protection and creating a significant legal gap.

Historically, the recognition of the relationship between environmental protection and human welfare progressed following the 1972 United Nations Conference on the Human Environment held in Stockholm [5]. The Stockholm Declaration established the fundamental principles that have shaped subsequent environmental governance and highlighted the human dimension of environmental degradation. Despite this progress, the legal and policy frameworks established since then have not kept pace with the rapidly increasing incidence of climate-induced displacement.

Furthermore, despite the evident scale of climate-induced displacement, the existing international legal framework inadequately addresses the rights and protections of those forced to move due to environmental reasons. Unlike other categories of forced displacement, such as refugees who are fleeing political persecution or armed conflict, individuals displaced by climate change

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.21>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

lack a clearly defined legal status and corresponding protections under international law. This legislative void exposes climate migrants to heightened vulnerabilities and legal precarity, underscoring the urgent need for a comprehensive legal framework that recognizes and safeguards their rights.

In addition to legal and policy dimensions, climate-induced migration is shaped by media discourse. Journalistic framing influences how displaced populations are represented, that is, as victims, threats, or rights-bearing subjects, thereby affecting public understanding and political responses. Media narratives thus function as a critical intermediary between environmental realities, legal debates and governance outcomes.

Understanding the nuances of this relationship, the corresponding legal frameworks and the role of media representations is crucial to address the vulnerabilities of climate-affected populations. In this regard, this paper seeks to critically examine gaps in the international legal framework relating to climate-forced migration, while also considering how media narratives shape public understandings of these gaps. By analyzing contemporary climate change impacts on migration patterns to the EU, relevant legal perspectives and dominant media framings, this study aims to formulate specific recommendations to enhance both the protection and support mechanisms for climate migrants and the quality of public discourse surrounding climate-induced mobility, thereby contributing to more just and effective global governance in the face of environmental displacement.

II. MATERIALS AND METHODS

This study applies a mixed-methods approach that combines quantitative analysis of secondary migration data with qualitative legal and policy analysis. The aim is to examine patterns of climate-induced migration towards the EU and to evaluate the adequacy of existing legal frameworks addressing such movements. This approach allows the study to combine statistical trends with legal and contextual analysis for a more comprehensive understanding of the issue.

Empirical data, primarily focused on the period between 2020-2025, was obtained from official sources, including Eurostat, the United Nations, the UNHCR, the Internal Displacement Monitoring Centre, the National Oceanic and Atmospheric Administration, and the Germanwatch Climate Risk Index. This part of the analysis focuses on identifying immigration trends of non-EU citizens and assessing potential links between environmental stressors and migration dynamics. The quantitative analysis identifies general patterns but does not establish direct causality.

The legal analysis followed a comparative approach, examining international and regional initiatives such as the 1951 Refugee Convention and the 1967 Protocol, as well as relevant human rights treaties and recent bilateral treaties. Soft law initiatives, including the Sendai Framework, the Nansen Initiative, and the Paris Agreement, were also considered. Case law from the International Court of Justice, the Inter-American Court of

Human Rights, and the European Court of Human Rights was also reviewed to identify emerging interpretations relevant to climate displacement. The Australia–Tuvalu Falepili Union Treaty was identified as a contemporary example of best practice in this area. In general, this analysis helps evaluate how legal frameworks address climate-induced migration in practice.

To complement the quantitative migration data and the comparative legal analysis, the study incorporates a literature-based examination of media narratives related to climate induced migration. This analysis is supplemented by illustrative examples from prominent European news outlets published between 2020 and 2025, in order to identify dominant framing patterns, terminological choices, sourcing practices, and strategies of contextualization as well as to assess the extent to which legal and human rights dimensions are reflected in public discourse. This qualitative analysis focuses on identifying common patterns rather than producing generalizable results.

The research is grounded in a rights-based framework that links climate justice, migration governance, and the protection of human rights. Although limited by the absence of a universal definition of “climate migrant” and reliance on secondary data, the study mitigates these constraints through triangulation of multiple sources and critical cross-comparison of empirical, legal and media-based evidence. Among of the key limitations of the selected methodological approach include reliance on secondary data, and predominantly interpretative nature of the qualitative analysis. The absence of primary data (e.g., interviews) may also limit insight into lived experiences. Despite this, the mixed-methods approach strengthens the overall analysis through triangulation.

III. RESULTS AND DISCUSSION

Climate change, alongside military conflicts, political instability, and socio-economic inequalities, is one of the key factors forcing people to migrate, often involuntarily. The multifaceted repercussions of rising global surface and ocean temperatures (see Figure 1) extend far beyond environmental degradation, encompassing profound natural, social, economic, and territorial implications. These consequences increasingly contribute to displacement, rendering climate change not merely an environmental crisis, but a catalyst for humanitarian emergencies.

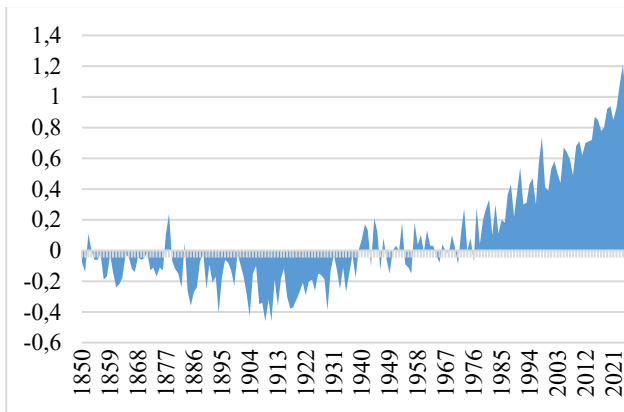


Fig. 1. Example of a figure caption. (Source: National Centers for Environmental Information, 2025)

The above figure shows a worrying climatological trend: a pronounced and sustained rise in the global average temperature since the beginning of the 21st century, particularly in comparison to the 1901–2000 baseline period. This marked deviation from historical temperature norms underscores the accelerating pace of anthropogenic climate change and signals the intensification of its associated impacts across both natural and human systems.

Among the most commonly observed manifestations of climate-induced stressors that cause human displacement are a significant reduction in the availability of potable freshwater resources, the forced migration or extinction of animal species, and a substantial rise in sea levels, which exacerbates the risk of coastal flooding and shoreline erosion. Moreover, the health-related consequences of climatic shifts, manifested in declining population health and increased occupational hazards, directly impact labor force availability and productivity, particularly in climate-sensitive sectors such as agriculture and construction. Infrastructure in vulnerable regions is frequently ill-equipped to withstand extreme weather events, further compounding the exposure of local populations to risk. Substantial declines in agricultural output, due in part to shifting precipitation patterns and increased incidences of drought and soil salinization, reduce the arability of land and diminish food security, thereby undermining the viability of traditional livelihoods and accelerating migratory pressures [6].

As environmental conditions deteriorate in many regions, resulting in resource scarcity, extreme weather events, and reduced habitability, people are increasingly compelled to seek better conditions in areas with more favorable climatic and socio-economic conditions. In this regard, the EU, which is usually associated with a relatively stable climate and high living standards, is a key destination for climate-induced migration. Figure 2 shows the total number of immigrants whose country of origin is not an EU Member State for the period 2020–2023.

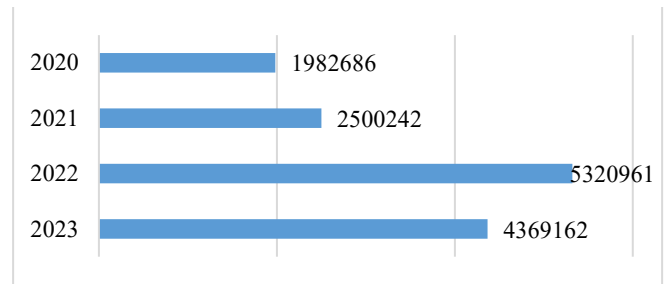


Fig. 2. Number of immigrants from non-EU countries (Source: Eurostat [7])

As can be seen from the data presented in Figure 2, there has been a marked increase in the inflow of migrants into the EU between 2020 and 2023. Notably, the data indicate a sharp peak in 2022, which can be primarily attributed to the Russian invasion of Ukraine. This armed conflict has triggered a substantial and rapid displacement of Ukrainian citizens, many of whom have been granted temporary protection within the EU. However, it is important to note that this surge in immigration to the EU cannot be attributed to climate change; rather, it is a consequence of geopolitical instability and armed conflict, thereby falling under the broader category of conflict-induced displacement.

To more accurately assess trends related to environmentally forced displacement, it is essential to distinguish such movements from those triggered by military conflicts or political persecution. In this regard, further insight can be gained by analyzing the countries of origin of the nationalities most frequently represented among immigrants in the EU (see Figure 3). Such an examination provides a clearer picture of the extent to which climate-related events are driving migration towards the EU.

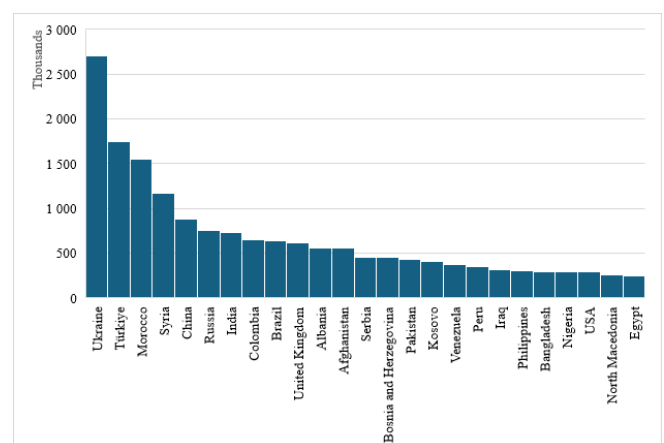


Fig. 3. Top nationalities of non-EU citizens that are usual residents in the EU as of 1 January 2024 (Source: Eurostat [8])

As illustrated in Figure 3, a predominant part of immigrants in the EU do not originate from countries that are most frequently affected by climate-related disasters. However, according to the Germanwatch [9] Climate Risk

Index (CRI), the major non-EU countries that feature the top 10 list of states most severely impacted by such disasters are China, India, and the Philippines. The CRI is a reliable and useful tool for such studies as its methodology evaluates the impact of extreme weather events, by incorporating indicators such as economic losses, mortality rates, and the number of people affected. From an economic perspective, climate-related disasters such as droughts, floods, heatwaves, storms, and wildfires resulted in estimated financial losses of approximately USD 44 billion in China, USD 20 billion in India, and USD 2.3 billion in the Philippines between 1993 and 2022.

Moreover, these three countries are not generally considered politically unstable, nor are they characterized by widespread civil conflict. This assessment is supported by the relatively low number of people forcibly displaced from these countries who seek asylum in Europe [10]. Consequently, it could be speculated that part of the nearly 900,000 Chinese, over 700,000 Indian, and approximately 300,000 Filipino residents in the EU may have immigrated for reasons directly or indirectly linked to climate change. These findings highlight the growing importance of addressing the legal status and protection gaps faced by individuals migrating due to environmental and climate-related factors – a topic that will be examined in greater detail in the following subsection.

A. Legal aspects of climate forced migration

The legal concept of ‘refugee’, to which their rights and protections are inextricably linked, stems from the 1951 UN Convention on the Status of Refugees, and their status from the 1967 New York Protocol. The definition adopted therein establishes a link between the refugee status and a “well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion” (Article 1(A)(2) of the UN Refugee Convention). This provision is, therefore, not directly applicable to ‘climate refugees’ [11], as the Convention was designed in the wake of the Second World War to define states’ obligations towards affected individuals. The possibility of people later being pressured to leave their home due to climate change (and the corresponding duties of other states towards these individuals) was not one of the foreseeable concerns of the Convention’s drafters.

However, the concept of ‘environmental refugees’ is not new. It has already been defined as “those people who have been forced to leave their traditional habitat, temporarily or permanently, because of a marked environmental disruption (natural and/or triggered by people) that jeopardized their existence and/or seriously affected the quality of their life. By ‘environmental disruption’ in this definition is meant any physical, chemical and/or biological changes in the ecosystem (or the resource base) that render it, temporarily or permanently, unsuitable to support human life.” [12]. Nevertheless, this is not a recognised category of refugees or even migrants for any legal purpose [13].

The legal response to this phenomenon is lacking at the moment; and it is also unlikely that an international treaty or protocol will be drafted in the near future. Firstly,

because the current historical moment is fraught with resistance to the acceptance of migrants (particularly in the Global North) – therefore, a new treaty establishing state obligations towards another category of refugees would be too contentious. Secondly, there is also no consensus on the legal response to be adopted: while some advocate the adoption of a treaty or additional protocol [14], others argue that adopting such a (misleading) concept would be a mistaken endeavor [15][16]. Nevertheless, some regional attempts have successfully established future responses to population displacement caused by climate change (such as in Pakistan and Australia).

As the effects of climate change worsen, new challenges and obstacles may arise in the adoption of a legal framework governing migration agreements. For example, if the entirety of a state’s territory becomes submerged and disappears, this could present a significant challenge. This issue is linked to the continuity or loss of sovereignty (as recognized in the recent International Court of Justice (ICJ) advisory opinion of 23 July 2025, para. 357), as the validity of an international treaty would require the sovereign power of all signatories. While some may still advocate that sovereignty requires a corresponding (land) territory over which to exert sovereign power – in a strict application of the Montevideo criteria –, a more nuanced approach allows for maintenance of sovereignty despite the disappearance of the physical territory. To deem otherwise would overburden small states (usually islands) with the consequences of a situation to which they contributed the least [17]. This is also the opinion of the ICJ, who stated that “once a State is established, the disappearance of one of its constituent elements would not necessarily entail the loss of its statehood” (para. 363 of the Advisory Opinion of 23 July 2025).

While it is true that no specific legislation concerning the category of ‘climate migrants/refugees’ exists, the need for a legal framework that may be applicable has led to many suggestions in this regard. International standards of protection of human rights must be the starting point [17] as environmental catastrophes often lead to human rights violations, some treaties may apply to these situations, regardless of the fact that people have migrated due to climate change. In this context, for example, the obligation not to deport someone may arise, given the prospective violation of their human rights in such a situation [18][19][20].

Another possibility that may be triggered is the (limited) application of refugee law. However, this would only occur when other factors that trigger asylum were also present in the situation [21][22]. The crisis in Sudan is a clear example of such a situation, where the successive climate-induced changes and resulting food insecurity have led to increased violence and instability in the region [23] – which, in turn, could trigger the application of refugee law. In addition to these possibilities, there are also soft law instruments that could provide guidance, such as the Sendai Framework for Disaster Risk Reduction, the Nansen Initiative, or even the Paris Agreement (for mapping, see [13]; [17]). Finally, some States are beginning to adopt agreements and measures – such as visas and humanitarian permits – designed to address climate-induced

displacement [17], and there is an increasing body of jurisprudence concerned with these circumstances [24][25][26].

Among the most recent examples of relevant jurisprudence is the case brought before the Interamerican Court of Human Rights [27], in which a connection was established between climate change and the responsibility of the state for particularly vulnerable individuals, including those deprived of their liberty. In such cases, special attention must be paid to the human rights of these individuals, as they are unable to simply leave the affected country or region and are, therefore, more susceptible to deteriorating detention conditions – including migrants detained while awaiting a decision on their cases (see especially para. 592 and 628 of the Opinion of the Court). In this context, it is also worth mentioning its European counterpart, the European Court of Human Rights (ECtHR), which has also evaluated climate-related cases, to establish the state's responsibility for its citizens. Although they are not related to migration, they may be relevant to the question of the procedural standing of individuals, given that the threshold for establishing victim status, as defined by the Court, is particularly high (see [28] and [29]).

The international scenario regarding climate-induced displacement may be currently bleak, but there are some positive aspects and good practices to highlight. One such example is the Falepili Union Treaty, between Tuvalu and Australia. This treaty is the first to specifically address climate-related displacement [30], establishing a resettlement scheme to provide security to Tuvalu's endangered population. The priority of the Australian government is to support the Tuvaluan efforts in staving off climate-induced changes; in parallel, relocation opportunities are offered (in yearly quotas) to Tuvaluan nationals who wish to settle in Australia, and they become eligible to apply for Australian citizenship. Other commendable aspects include the fact that this visa, which is accessible from anywhere in the world, provides a safe and legal route for Tuvaluans to flee increasingly dire living conditions; envisions the right to reside indefinitely in Australia, with unlimited freedom to travel to Tuvalu; it is not limited to people with specific skills; and it encompasses vulnerable people (e.g., due to age or disabilities). In return, Australia has a de facto veto power over Tuvaluan agreements with third states in certain areas, such as security and defense. This is understandable, given that Australia is obliged to provide Tuvalu with security (and is concerned with countering China's influence in the region – for an analysis, see [17]).

B. Media Narratives of Climate-Induced Migration

Media play a central role in shaping public discourse on climate-induced migration. In fact, for many people around the world, journalistic narratives constitute the main window through which they encounter environmental displacement and the experiences of affected populations [31]. This influence operates through framing practices, that is, the editorial choices journalists and media organizations make regarding what to emphasize or omit,

including terminology, sources and interpretive angles. These decisions shape whether climate-induced migrants are portrayed as security threats or vulnerable victims [30], often obscuring the structural inequalities and systemic drivers that underpin displacement [33][34].

Such framing patterns are not limited to climate-induced migration; they have been widely documented in journalistic coverage of migration and asylum more broadly [35][36][37]. In this respect, media narratives do not simply mirror social reality. Rather, they play an active role in shaping the political and legal frameworks within which responses to climate-induced displacement are debated and ultimately formulated.

Recent scholarship on media and climate-induced migration identifies two dominant framing patterns. The first is the security or crisis frame. Within this perspective, climate-related mobility is linked to border pressure, threats to social cohesion or strain on national welfare systems. In various media contexts, including Europe, the United States and Australia [38], migration is presented as a security consequence of climate change. News narratives often draw direct connections between climate-related disasters, resource shortage, conflict, instability and large-scale population movements [32]. In this framework, the “climate-driven refugee” is constructed as a monolithic and potentially destabilizing figure [32].

Indicative headlines from major international outlets illustrate how crisis- and security-oriented framing materializes in practice. Titles such as “Is the world ready for mass migration due to climate change?” [39] in BBC and “The climate refugee crisis is landing on Europe's shores – and we are far from ready” [40] in Politico Europe foreground scale, urgency and political destabilization, thereby reinforcing a securitized understanding of climate mobility.

A second dominant pattern is the humanitarian or vulnerability frame. This perspective foregrounds the suffering of populations affected by droughts, floods, sea-level rise and other extreme weather events. Within this framework, displaced individuals are primarily depicted as victims of climate change, passive and powerless figures in need of rescue or assistance [32]. While such representations may evoke empathy and humanitarian concern, they also tend to individualize suffering and direct attention toward immediate hardship rather than toward the structural drivers of displacement. In doing so, it obscures broader dynamics such as global inequalities, the unequal historical and political responsibility for environmental harm (e.g. greenhouse-gas emissions) and deeper questions of rights and climate justice [32].

At the same time, headlines such as “Flooding and droughts drove them from their homes. Now they're seeking a safe haven in New York” [41] in The Guardian foreground environmental suffering while simultaneously relocating the narrative to a major Western urban center. In doing so, they combine humanitarian victimization with an implicit focus on destination societies, illustrating how vulnerability framing may coexist with latent concerns

about reception, capacity and territorial impact. Such hybrid constructions demonstrate that humanitarian and security logics are not mutually exclusive but frequently intertwined within the same narrative structure. This convergence reflects what Bettini [33] describes as the dominance of apocalyptic narratives in climate-induced migration discourse, in which both humanitarian and security framings ultimately depoliticize the issue by presenting displacement as an inevitable crisis rather than as a politically produced condition embedded in global power relations.

This interplay raises a broader analytical question: how are these frames constructed? Through which journalistic mechanisms do they take shape? Frames are not abstract categories; they are produced through concrete editorial choices. Contextualization shapes meaning, determining whether displacement is presented as an isolated event or as part of broader structural and historical processes. Language plays a central role, as specific terms can signal crisis, threat or vulnerability. The selection of sources also matters, as political actors, security experts, humanitarian organizations or affected individuals each bring different perspectives and priorities. Finally, the way a story defines the problem and proposes solutions, whether in terms of border control, emergency relief or climate justice, contributes decisively to reinforcing particular framing patterns.

One of the most visible mechanisms through which these framing dynamics operate is the episodic nature of media coverage. Journalistic attention tends to intensify in the aftermath of extreme weather events, such as major wildfires, floods, hurricanes or during international climate summits, but often declines once the immediate crisis recedes. Consequently, climate-induced mobility is represented in episodic terms, tied to spectacular moments of disaster, rather than as an ongoing and structurally embedded phenomenon.

This episodic logic contributes to processes of dehumanization. When coverage is centered primarily on dramatic events, affected populations are frequently portrayed as anonymous masses or statistical figures, rather than as individuals with agency, histories and rights. The absence of sustained reporting limits deeper contextualization and reinforces simplified narratives that either dramatize crisis or reduce displacement to humanitarian emergency, without acknowledging the complex social political and economic conditions that shape mobility.

This episodic and disaster-centered logic becomes particularly visible in headlines that foreground immediate death tolls and large-scale displacement figures. Titles such as “At least 68 people killed in flooding as rains worsen Sudan’s plight” [42] in *The Guardian* and “Climate disasters displaced 250 million people in past 10 years, UN report finds” [43], also in *The Guardian*, prioritize casualty counts and aggregate statistics, frequently anchored in institutional sources. While such reporting conveys scale and urgency, it simultaneously abstracts affected populations into numerical categories. Individuals are rendered as counted bodies rather than narrated subjects,

reinforcing a mode of visibility in which climate mobility appears as a sudden humanitarian surge rather than as a structurally embedded and politically mediated process.

Within this episodic and decontextualized environment, language and the words journalists choose, constitute a central arena in which the politics of climate mobility unfolds, precisely because terminology is not merely descriptive; it carries normative and legal implications. This creates a tension: despite the absence of explicit recognition of climate related displacement under existing international refugee law, scholarship shows that media discourse more frequently employs the term “climate refugees” rather than “climate migrants” [44][45]. This preference is not neutral, as the label “refugee” carries strong moral and emotional resonance, conveying vulnerability and an implicit entitlement to protection. Headlines such as “The first internal climate refugees” in the Greek newspaper *Kathimerini* [46], referring to displaced populations after a natural disaster in central Greece, illustrate how this terminology amplifies humanitarian urgency. Yet this framing also produces a representational - legal mismatch: while morally powerful, the term ‘climate refugees’ does not align with established legal definitions, potentially shaping expectations of protection whose scope and applicability remain legally and politically unsettled.

A further crucial element concerns the selection of sources. Research indicates that media coverage frequently privileges institutional voices, such as political elites and government officials, while marginalizing the perspectives of affected communities. As Høeg et al.’s [47] study of BBC coverage demonstrates, individuals affected by climate induced displacement are more often spoken about than spoken with, a pattern that significantly constrains their represented agency. The predominance of institutional sources reinforces top-down narratives and contributes to portrayals in which displaced populations appear as objects of policy intervention rather than as subjects with political voice and lived experience.

This marginalization of lived experience is closely linked to the limited visibility of justice-oriented perspectives in mainstream coverage. The rights-based frame remains comparatively underrepresented and empirical research drawing on journalists’ own accounts confirms the structural and professional constraints that hinder the integration of rights-based perspectives into routine news production [48]. Yet this frame is normatively significant. It seeks to reposition climate-induced migration within broader debates on climate responsibility, structural inequality and human rights. From this standpoint, displacement is not treated as an unfortunate by-product of natural processes but as a foreseeable and unjust consequence of uneven development and the disproportionate environmental harm caused by historically high-emitting states. Climate justice, in this sense, entails recognition of the rights of vulnerable communities and the corresponding responsibilities of those who have contributed most to climate change [49].

Taken together, these patterns reveal that media narratives do not merely report on climate-induced

migration but actively structure how it is understood, debated and governed. The predominance of security and humanitarian framings, combined with the marginalization of justice-oriented perspectives, ultimately shapes the boundaries of political imagination within which climate mobility is rendered either a crisis to be managed or a responsibility to be collectively addressed.

IV. CONCLUSION

Even though Australia's Treaty with Tuvalu applies only to Tuvaluan nationals (and not to people of other nationalities migrating for the precise same reasons), it is still an outstanding example for future (worldwide) consideration. It has been recognized that climate change disproportionately impacts those countries that have contributed least to the problem and the multiple issues it creates (see [27]), which brings to the fore the need to provide safe migration paths for the people ultimately affected by sudden environmental catastrophes, as highlighted in the Global Compact for Migration (objective 5).

On the one hand, the duties to cooperate in addressing the issue and accommodate displaced people have been emphasized, particularly by Portugal and the Netherlands, in the context of the recent ICJ advisory opinion (in the oral and written submissions [50][51]). On the other hand, there may also be duties connected to assisting the affected population stay in their countries, namely by providing financial and/or technological assistance [52][53]. Both aspects have, in fact, been mentioned in the Pacific Regional Framework on Climate Mobility [54], as focusing exclusively or predominantly on the duty to relocate could exacerbate the losses and burdens of those wishing to remain in their home territory.

As most displacement caused by climate change or environmental disasters is predicted to be internal [55], current approaches are mainly regional for the time being, staving off the need for an immediate global response to the issue. Africa, Latin America and the Pacific are the regions that have engaged the most with the issue, with Africa leading the way in terms of the most progressive legal frameworks concerning climate change [56]. A stellar example of this is the IGAD Protocol on Free Movement of Persons [57], which applies to climate-induced migration (but has not yet come into force). However, as habitable conditions worsen, particularly in certain parts of the world, states will eventually need to design a long-term strategy to address the effects of climate change on the population, particularly because of their respective contributions to the problem and their share of responsibility for mitigating the most negative consequences. Given the (at least, moral) duty of states to answer for the consequences of their climate-harming behavior, the way forward must encompass climate-induced migration within an applicable legal framework that considers a humanitarian and solidarity-based perspective.

Therefore, future global legal approaches should envisage safe migration pathways to ensure the survival of

affected populations, acknowledge the duty to cooperate with affected states by accommodating displaced people and/or helping impacted populations to stay in their country, and recognize their responsibility by imposing clear duties towards affected people who may find themselves deprived of their homes and livelihoods due to climate change.

At the same time, the effectiveness and legitimacy of future legal responses will depend not only on normative developments but also on the ways in which climate-induced migration is framed in public discourse. As this study has shown, dominant security and humanitarian narratives often overshadow justice-oriented perspectives, thereby shaping the boundaries within which political responsibility is imagined. A more balanced and rights-based media representation may therefore play a crucial role in fostering the solidarity and long-term commitment required for meaningful legal reform.

ACKNOWLEDGMENT

This paper presents results obtained as part of the project KII-06-M85/1 "Refugee Processes: Socio-Economic Dimensions in the Contemporary Security Environment", funded by the Bulgarian National Science Fund.

REFERENCES

- [1] United Nations. (2025). Causes and Effects of Climate Change. Retrieved from <https://www.un.org/en/climatechange/science/causes-effects-climate-change>.
- [2] Internal Displacement Monitoring Centre (IDMC). (2019). Global Report on Internal Displacement. Retrieved from <https://www.internal-displacement.org/global-report/grid2019/>.
- [3] National Oceanic and Atmospheric Administration (NOAA). (2025). Climate Change Impacts. Retrieved from <https://www.noaa.gov/education/resource-collections/climate/climate-change-impacts>.
- [4] International Organization for Migration (IOM). (2023). Let's Talk About Climate Migrants, Not Climate Refugees. Retrieved from <https://lac.iom.int/en/blogs/lets-talk-about-climate-migrants-not-climate-refugees>.
- [5] United Nations. (1972). Declaration of the United Nations Conference on the Human Environment, Stockholm. Retrieved from <https://www.un.org/en/conferences/environment/stockholm1972>.
- [6] European Commission. (2025). Consequences of climate change. Retrieved from https://climate.ec.europa.eu/climate-change/consequences-climate-change_en.
- [7] Eurostat. (2024). Migration and asylum in Europe – 2024 edition. Retrieved from <https://ec.europa.eu/eurostat/web/interactive-publications/migration-2024>.
- [8] Eurostat. (2025). EU population diversity by citizenship and country of birth. Retrieved from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_population_diversity_by_citizenship_and_country_of_birth#:~:text=Ukrainian%2C%20Turkish%20and%20Moroccan%20citizens,younger%20than%20native%20born%20persons.
- [9] Germanwatch. (2025). Climate Risk Index 2025. Retrieved from: <https://www.germanwatch.org/en/cr/>.
- [10] Eurostat. (2025a). Asylum applicants by type, citizenship, age and sex - annual aggregated data. Retrieved from: https://ec.europa.eu/eurostat/databrowser/view/migr_asyappctza/default/table?lang=en

- [11] D'Orsi, C. and Naldi, G. J. (2022). "Climate-induced displacement in the Sahel: A question of classification". *International Review of the Red Cross* 103, pp. 1029-1065. <https://doi.org/10.1017/S1816383121000941>
- [12] El-Hinnawi, E. (1985). *Environmental Refugees*. United Nations Environment Programme. Nairobi.
- [13] Teles, P. G. (2023). "The "Human Face" of Sea Level Rise: Protection of persons Affected". *American University International Law Review* 38(3), pp. 693-700.
- [14] Fry, I. (2023). "Providing legal options to protect the human rights of persons displaced across international borders due to climate change. Report of the Special Rapporteur on the promotion and protection of human rights in the context of climate change". Human Rights Council, Fifty-third session. Available at: <https://www.ohchr.org/en/documents/thematic-reports/ahrc5334-providing-legal-options-protect-human-rights-persons-displaced>
- [15] McAdam, J. (2011). "Swimming against the Tide: Why a Climate Change Displacement Treaty is Not the Answer". *International Journal of Refugee Law* 23(1), pp. 2-27. <https://doi.org/10.1093/jlrl/eeq045>
- [16] Abate, R. S. and Bhardwaj, C. (2024). "Enhancing Protection of "Climate Refugees" in Destination Hubs: A Comparative Analysis of Legal Mechanisms and Governance Challenges in the United States and India". *Harvard Human Rights Journal* 37(2), pp. 293-318.
- [17] Ardito, E. (2024). "Sinking States" open questions: Continuity of statehood and human rights protection of forcibly displaced people. The case of Tuvalu in light of the Falepili Union Treaty". *Asomare Yearbook on the Law of the Sea* 4, pp. 481-504.
- [18] UN Human Rights Committee. (2020). *Ioane Teitiota v. New Zealand*. Communication No. 2728/2016, Decision of 7 January 2020.
- [19] Rive, V. (2020). "Is an Enhanced Non-refoulement Regime under the ICCPR the Answer to Climate Change-related Human Mobility Challenges in the Pacific? Reflections on Teitiota v New Zealand in the Human Rights Committee". *Questions of International Law* 75, pp. 7-24.
- [20] Maneggia, A. (2020). "Non-refoulement of Climate Change Migrants: Individual Human Rights Protection or 'Responsibility to Protect'? The Teitiota Case Before the Human Rights Committee". *Diritto umani e diritto internazionale* 2/2020, pp. 635-643.
- [21] McAdam, J. (2022). "Moving beyond Refugee Law: Putting Principles on Climate Mobility into Practice". *International Journal of Refugee Law* 34(3-4), pp. 440-448.
- [22] United Nations High Commissioner for Refugees (UNHCR). (2020). *Legal considerations regarding claims for international protection made in the context of the adverse effects of climate change and disasters*. 1 October 2020.
- [23] Stromsta, R. (2025). "Escalating Crisis, Rising Floods: Insecurity, Conflict, and Displacement in South Sudan". *Researching Internal Displacement*, Post of 6 November 2025. Available at: https://researchinginternaldisplacement.org/short_pieces/escalating-crisis-rising-floods-insecurity-conflict-and-displacement-in-south-sudan/
- [24] Kaminski, I. (2025). "There's no legal definition of a climate refugee - does that matter?". Available at: <https://www.the-wave.net/legal-definition-climate-refugee/>
- [25] Constitutional Court of Colombia. (2024). *Sentencia No. T-123*. 16 April 2024.
- [26] González, F. (2022). *Informe del Relator Especial sobre los derechos humanos de los migrantes, Felipe González, A/77/189*. 19 July 2022.
- [27] Interamerican Court of Human Rights. (2025). *Opinión Consultiva OC-32/25 de 29 de Mayo de 2025 Solicitada por la República de Chile y la República de Colombia. Emergencia Climática y Derechos Humanos*. Available at: <https://corteidh.or.cr/tablas/OC-32-2025/>
- [28] European Court of Human Rights (ECtHR). (2024). *Verein KlimaSeniorinnen Schweiz and Others v. Switzerland*. Application no. 53600/23. 9 April 2024.
- [29] Heri, C. (2025). "Climate-related vulnerabilities and the European Court of Human Rights: Reimagining victim status through intersectional thinking". *Leiden Journal of International Law*, First View, (2025), pp. 1-24. DOI: Guilfoyle <https://doi.org/10.1017/S0922156525100502>
- [30] Guilfoyle, D. and Green, A. (2023). "The Australia-Tuvalu Falepili Union Treaty: Security in the Face of Climate Change...and China?" (28 November 2023) *EJIL:TALK!*. Available at: <https://www.ejiltalk.org/the-australia-tuvalu-falepili-union-treaty-security-in-the-face-of-climate-change-and-china/>
- [31] Schafer, M.S. (2015). *Climate change and the media*. In: Wright JD (ed.) *International Encyclopedia of the Social & Behavioral Sciences*. Oxford: Elsevier, pp.853-859.
- [32] Sakellari, M. (2021). *Media coverage of climate change induced migration: Implications for meaningful media discourse*. *Global Media and Communication*, 18(1), 67-89. <https://doi.org/10.1177/17427665211064974>
- [33] Bettini, G. (2013). *Climate change barbarians at the gate? A critique of apocalyptic narratives on 'climate refugees'*. *Geoforum* 45: 63-72.
- [34] Hartmann, B. (2010). "Rethinking climate refugees and climate conflict: Rhetoric, reality and the politics of policy discourse", *Journal of International Development*, 22(2), pp. 233-246.
- [35] Benson, R. (2013). *Shaping immigration news: A French-American comparison*. Cambridge University Press.
- [36] Kalfeli, P., Angeli, C., & Frangonikolopoulos, C. (2024). *Victims of a human tragedy or "objects" of migrant smuggling? Media framing of Greece's deadliest migrant shipwreck in Pylos' dark waters*. *Journalism and Media*, 5(2), 537-551. <https://doi.org/10.3390/journalmedia5020036>
- [37] Van Gorp, B. (2005). *Where is the frame? Victims and intruders in the Belgian press coverage of the asylum issue*. *European Journal of Communication*, 20(4), 484-507. <https://doi.org/10.1177/0267323105058253>
- [38] Schäfer M, Scheffran J and Penniket L (2016) *Securitization of media reporting on climate change? A cross-national analysis in nine countries*. *Security & Dialogue* 47(1): 76-96.
- [39] Vince, G. (2022, November 18). *Is the world ready for mass migration due to climate change?* BBC Future. <https://www.bbc.com/future/article/20221117-how-borders-might-change-to-cope-with-climate-migration>
- [40] Özdemir, I. (2023). *The climate refugee crisis is landing on Europe's shores – and we are far from ready*. Politico Europe. <https://www.politico.eu/article/climate-refugee-crisis-europe-policy/>
- [41] Jiwa, J., & Mandiola, C. (2025, October 22). *Flooding and droughts drove them from their homes. Now they're seeking a safe haven in New York*. The Guardian. <https://www.theguardian.com/environment/2025/oct/22/climate-disasters-migration-new-york>
- [42] The Guardian. *At least 68 people killed in flooding as rains worsen Sudan's plight*. <https://www.theguardian.com/world/article/2024/aug/14/sudan-flooding-rains-civil-war-conflict-famine>
- [43] Lakhani, N. (2025, November 9). *Climate disasters displaced 250 million people in past 10 years, UN report finds*. The Guardian. <https://www.theguardian.com/environment/2025/nov/09/climate-disasters-displaced-250-million-people-in-past-10-years-un-report-finds>
- [44] Bonneux, I. & Van Praag, L. (2024) *Millions of climate refugees are coming!* A critical media discourse analysis on climate change-induced migrants in Flemish press, *Environmental Sociology*, 10:4, 486-498, <https://doi.org/10.1080/23251042.2024.2369738>
- [45] Casagrande, M. (2017). *Migrants or refugees? The discursive representation of climate-induced migration on BBC News Online*. *Anglistica AION*, 21(2), 37-53.
- [46] Kathimerini. (2023, October 2). *"The first internal climate refugees"*. Ekathimerini. <https://www.ekathimerini.com/multimedia/images/1221349/the-first-internal-climate-refugees/>

- [47] Høeg, E., & Tulloch, C. D. (2018). Sinking Strangers: Media Representations of Climate Refugees on the BBC and Al Jazeera. *Journal of Communication Inquiry*, 43(3), 225-248. <https://doi.org/10.1177/0196859918809486>
- [48] Kalfeli, P., Angeli, C., & Frangonikolopoulos, C. (2025). Through their eyes: Journalists' perspectives on framing, bias, and ethics in media coverage of minorities. *Journalism and Media*, 6(3), 98. <https://doi.org/10.3390/journalmedia6030098>
- [49] Bulkeley, H., Carmin, J., Castán Broto, V., Edwards, G. A. S., & Fuller, S. (2013). Climate justice and global cities: Mapping the emerging discourses. *Global Environmental Change*, 23(5), 914–925. <https://doi.org/10.1016/j.gloenvcha.2013.05.010>
- [50] International Court of Justice (ICJ). (2024a). Public sitting held on Tuesday 10 December 2024, at 3 p.m., at the Peace Palace, President Salam presiding, on the Obligations of States in respect of Climate Change (Request for advisory opinion submitted by the General Assembly of the United Nations). Available at: <https://www.icj-cij.org/sites/default/files/case-related/187/187-20241210-ora-02-00-bi.pdf>
- [51] International Court of Justice (ICJ). (2024b). Obligations of States in Respect of Climate Change (Request for an Advisory Opinion). Written Statement of the Kingdom of the Netherlands. Available at: <https://icj-cij.org/sites/default/files/case-related/187/187-20240321-wri-14-00-en.pdf>
- [52] McAdam, J. and Wood, T. (2023). Kaldor Centre Principles on Climate Mobility. Available at: https://www.unsw.edu.au/content/dam/pdfs/unsw-adobe-websites/kaldor-centre/2023-11-others/2023-11-Principles-on-Climate-Mobility_v-4_DIGITAL_Singles.pdf
- [53] McAdam, J., Jefferies, R., and Mulder, T. (2025). “The Real Disaster May Only Just be Beginning for Those Displaced by Hurricane Melissa”. *Researching Internal Displacement*, Post of 4 November 2025. Available at: https://researchinginternaldisplacement.org/short_pieces/the-real-disaster-may-only-just-be-beginning-for-those-displaced-by-hurricane-melissa/
- [54] Pacific Islands Forum. (2024). Pacific Regional Framework On Climate Mobility. Available at: <https://www.pacificclimatechange.net/sites/default/files/document/s/2024%20Pacific%20Regional%20Framework%20on%20CM.pdf>
- [55] Internal Displacement Monitoring Centre (IDMC). (n.d.). Displacement, disasters and climate change. Available at: <https://www.internal-displacement.org/focus-areas/Displacement-disasters-and-climate-change/?ref=the-wave.net>
- [56] Mbiyozo, A.-N. and Wood, T. (2025). “Turning Africa’s legal advantages into benefits for climate refugees”. *Institute for Security Studies*, 24 February 2025. Available at: <https://issafrica.org/iss-today/turning-africa-s-legal-advantages-into-benefits-for-climate-refugees?ref=the-wave.net>
- [57] IGAD Protocol on Free Movement of Persons. (2020). Available at: <https://migrationnetwork.un.org/policy-repository/igad-protocol-free-movement-persons>

Physical Vulnerability of Cyber Systems: Analysis of Incidents, Risk Factors and Security Strategies

Nikolay Penev

University of Library Studies and
Information Technologies
Sofia, Bulgaria
4623496-2@unibit.bg

Daniela Pavlova

Faculty of Information Sciences,
Computer Sciences Department
University of Library Studies and
Information Technologies
Sofia, Bulgaria
d.pavlova@unibit.bg

Jasen Tanev

University of Library Studies and
Information Technologies
Sofia, Bulgaria
q.tanev@unibit.bg

Nikolay Koev

University of Library Studies and
Information Technologies
Sofia, Bulgaria
4623497-2@unibit.bg

Andrian Stoilov

University of Library Studies and
Information Technologies
Sofia, Bulgaria
a.stoilov@unibit.bg

Kiril Nikolov

University of Library Studies and
Information Technologies
Sofia, Bulgaria
k.nikolov@unibit.bg

Abstract—Physical security is an essential component of cybersecurity risk management because many cyber and operational technology systems depend on protected facilities, equipment, power supply, communication links and environmental conditions. This paper revises the analysis of physical vulnerability in cyber systems by distinguishing direct physical compromise from cyber incidents that produce physical consequences. A qualitative incident-based methodology is applied to selected cases from 2020 to 2024 and to recent cyber-physical security literature. The method includes source screening, inclusion and exclusion criteria, incident coding by physical vector, affected asset, impact and dependency, and a reproducible ordinal risk score. The results systematize incidents into five categories: direct physical attacks on infrastructure, environmental disruption, compromise of physical-security platforms, compromise of operational technology with physical consequences, and hybrid cyber-physical scenarios. The paper proposes a methodological framework for assessing such incidents and maps the main risk factors to practical security strategies. The findings show that physical vulnerability should not be reduced to facility protection alone; it should be treated as a combined governance, engineering and incident-response problem linking physical access, operational technology, cyber monitoring and business continuity.

Keywords—Critical Infrastructure Protection, Cyber-Physical Systems, Physical Vulnerability, Risk Assessment.

I. INTRODUCTION

The increasing integration of physical security systems, cyber infrastructure and operational technology (OT) has created a class of risks that cannot be assessed only through conventional information-security controls. Facilities, sensors, actuators, cameras, access-control systems, building automation platforms and industrial control systems are now connected to networks and cloud services, while their failure can affect physical processes and public services. The World Security Report 2023 shows that many security executives already perceive cyber threats against physical security systems as a major organizational challenge [1].

In this paper, a physical vulnerability of a cyber system is defined as a weakness related to physical access, physical protection, equipment location, environmental dependency, power supply, communication infrastructure, or cyber-physical interface that can affect the confidentiality, integrity, availability, safety, or continuity of a digital, OT, or cyber-physical system. This definition is consistent with the NIST view of OT as systems and devices that interact with, monitor, or control the physical environment [2].

Recent scientific literature also emphasizes that cyber-physical system (CPS) security requires threat and risk assessment approaches that connect the cyber domain with the physical domain. Systematic reviews and surveys highlight the importance of defense mechanisms,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.58>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

dependency modelling, safety-security integration and risk prioritization in industrial CPS and OT environments [3]-[6]. However, many incident-based discussions still mix direct physical vulnerabilities with general cyberattacks, ransomware, social engineering and insider threats. This weakens the analytical value of the categorization.

The aim of this study is to provide an incident-based assessment of physical vulnerabilities in cyber systems and to propose a reproducible methodological framework for classifying incidents, evaluating risk factors and selecting mitigation strategies. The contribution of the paper is threefold. First, it clarifies the difference between direct physical compromise and cyber incidents with physical consequences. Second, it systematizes selected incidents according to year, target, vector, impact and risk score. Third, it proposes a methodological framework that can support future assessment of physical security breaches affecting cyber, OT and cyber-physical systems.

II. MATERIALS AND METHODS

A. Research Scope and Definitions

The study applies a qualitative incident-based research design. It does not claim to be a full statistical survey of all physical-security incidents. Instead, it uses selected documented incidents and authoritative reports to develop a structured assessment framework. The analysis covers incidents and cyber-physical scenarios from 2020 to 2024, while the supporting literature includes peer-reviewed and institutional sources relevant to CPS, OT and critical infrastructure security.

The analysis distinguishes three related but different cases. Direct physical vulnerability refers to physical access, sabotage, theft, environmental damage, or failure of physical protection that directly affects cyber or OT assets. Cyber compromise with physical consequences refers to a cyber intrusion into OT or control systems that can affect physical processes, even when the initial intrusion is not physical. Human-factor incidents such as social engineering are not treated as physical vulnerabilities unless they are directly connected to physical access control, facility security or device compromise.

B. Source Selection and Screening

Sources were selected from four groups: peer-reviewed literature on CPS and OT security, institutional guidance from NIST and CISA, public incident reports, and official or organization-level incident descriptions. Selected sectoral and incident sources were used to document cases relevant to energy infrastructure, environmental disruption, security platforms, building automation, water treatment, and ICS/OT attacks [9]-[14].

Incidents were included when at least one of the following conditions was met: a direct physical act affected a cyber or OT asset; an environmental event disrupted the physical dependencies of cyber infrastructure; a physical-security platform was compromised; an OT or ICS system was compromised with potential physical consequences; or a controlled cyber-physical test demonstrated a combined attack path. Incidents were excluded from the core sample

when no physical component or physical consequence could be identified from public evidence. For this reason, general ransomware or social-engineering cases were not used as core examples unless they were connected to physical access or OT operation.

C. Incident Coding and Risk Scoring

Each incident was coded according to the following variables: year, sector, target, physical or cyber-physical vector, affected cyber/OT asset, operational impact, evidence type and mitigation focus. To make the comparison reproducible, a simple ordinal risk score was used:

$$R = E \times I \times D \quad (1)$$

where E is exposure, I is impact and D is dependency. Each variable is scored from 1 to 5 and the risk score is calculated according to (1). Exposure reflects how reachable or weakly protected the relevant physical or OT asset is. Impact reflects the potential operational, safety, continuity, or data-security effect. Dependency reflects the degree to which other services depend on the affected asset. For transparency, the ordinal scale is interpreted as follows: 1 = low, isolated, or minimal effect; 3 = moderate exposure, sector-level disruption potential, or medium dependency; 5 = high exposure, severe operational/safety effect, or strong dependency of critical services on the affected asset. Scores 2 and 4 represent intermediate levels between the defined low, moderate and high categories.

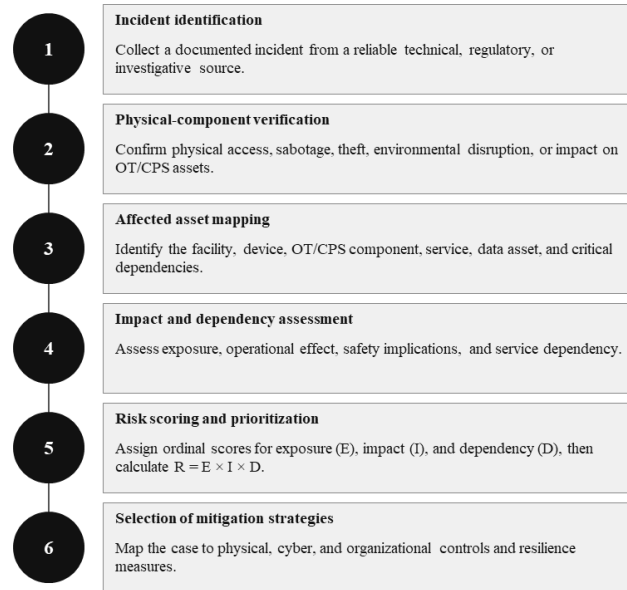


Fig. 1. Methodological framework for assessing incidents caused by physical vulnerabilities of cyber systems.

The framework in Fig. 1 starts with the identification of an incident and then verifies whether a physical component is present. If the case is only a cyber incident without a physical element, it is excluded from the physical-vulnerability category or treated as a related cyber-to-physical case. The next step maps the affected asset and its dependencies, followed by risk scoring. The final steps map the incident to security strategies and use the lessons

learned to improve response, recovery and governance processes. The framework is aligned with the logic of the NIST Cybersecurity Framework 2.0 functions - Govern, Identify, Protect, Detect, Respond and Recover [7] - and with CISA cross-sector goals for prioritized practices in IT and OT environments [8].

III. RESULTS AND DISCUSSION

A. Incident Categorization

The incident analysis shows that physical vulnerability in cyber systems is not a single category. Five analytical categories were identified: direct physical attacks on infrastructure; environmental hazards affecting cyber or

OT dependencies; unauthorized access or compromise of physical-security platforms; OT or building automation compromise; and cyber-to-physical boundary cases. The summarized incident coding is presented in Table 1. The cases also show that physical and cyber impacts often interact. A substation shooting can cause digital service disruption because communication, control and business operations depend on power. A compromised cloud-based camera platform may expose physical-security data even though the intrusion path is digital. A water-treatment attack may begin remotely but create potential physical process effects. Therefore, the analytical distinction between vector and consequence is essential.

TABLE 1 SUMMARY OF SELECTED INCIDENTS AND ORDINAL RISK CODING.

Year	Incident / sector	Target / affected asset	Method / vector	Impact / consequence	Risk R (E/I/D)
2020	Glass Fire, California / infrastructure dependencies [10]	Power, facility and communication dependencies	Environmental physical disruption	Availability and continuity risk for dependent systems	32 (2/4/4)
2021	Verkada platform compromise / physical-security systems [11]	Video surveillance and access-control platform	Compromise of a physical-security platform	Camera-feed exposure and facility-related information risk	36 (4/3/3)
2021	Building automation attack, Germany / BMS [12]	Building automation and facility-control devices	Compromise of automation devices	Loss of contact with devices and operational disruption	48 (4/3/4)
2021	Oldsmar water treatment / water sector [13]	Water-treatment process control interface	Unauthorized remote access; cyber-to-physical case	Potential manipulation of water-treatment process	75 (5/5/3)
2022	Moore County substations / energy sector [9]	Electrical substations and dependent services	Firearms attack against substations	Power outage and disruption of dependent digital services	60 (3/5/4)
2023-2024	Cyber Av3ngers and pro-Russia ICS attacks / water, food, healthcare [14]	Internet-facing PLC/HMI and OT assets	PLC/HMI compromise affecting physical processes	Manual operations, HMI manipulation and service-continuity risk	80 (5/4/4)

Note: E - exposure; I - impact; D - dependency; R - ordinal risk score. The notation R (E/I/D) reports the final risk score and the three component scores. Scores are used for transparent prioritization, not for statistical probability estimation.

The evolution of selected incidents and developments is summarized in Fig. 2.

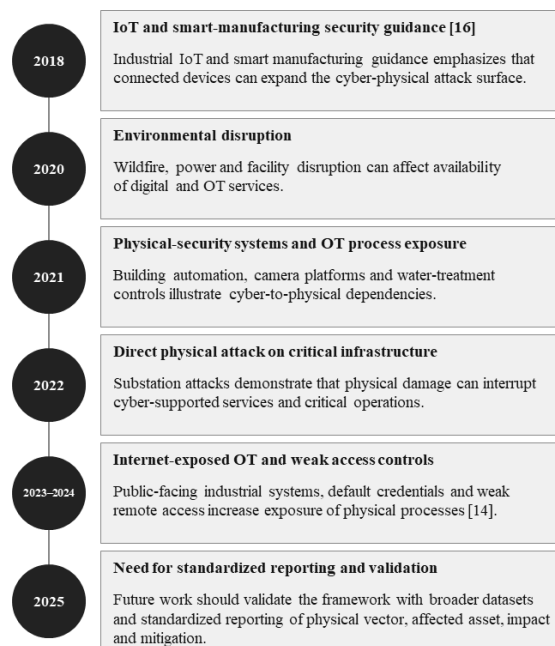


Fig. 2. Timeline of selected physical-security-related and cyber-physical incidents and developments, 2018-2025.

B. Interpretation of the Incident Evidence

The highest risk scores in Table 1 are associated with OT and ICS exposure because the affected systems can interact directly with physical processes. The ODNI/CTIIC dataset from November 2023 to April 2024 reports that Iran-affiliated and pro-Russia actors gained access to or manipulated U.S. ICS in several sectors, including water and wastewater, food and agriculture, healthcare and state/local government. The same report identifies poor password security, default credentials, outdated software and public-facing interfaces as important weaknesses [14].

Direct physical attacks remain highly relevant. The Moore County substation attack illustrates how physical damage to electrical infrastructure can disrupt services for a large population and affect dependent communications, business processes and digital systems. The NCSL report notes that physical security incidents against U.S. electricity infrastructure increased in 2022 compared with prior years and that reported incidents include vandalism, theft, suspicious activity, threats and trespassing [9].

Environmental hazards represent a different mechanism. They do not involve a malicious actor, but they can affect the physical dependencies of cyber systems: power supply, cooling, connectivity and facility availability. The Glass Fire is therefore treated not as a

cyberattack but as an example of environmental disruption that can undermine the operational continuity of dependent digital and cyber-physical services [10].

The Verkada case is also not a direct physical intrusion into a facility. Its relevance lies in the fact that the compromised system was a physical-security platform. Exposure of video feeds and facility-related data may support reconnaissance, privacy violations or subsequent physical-security risks [11]. Similarly, building automation incidents demonstrate that connected BMS devices can become an attack surface affecting lighting, access, heating, ventilation and other physical operations [12].

C. Risk Factors and Security Strategies

The analyzed incidents identify recurring risk factors: insufficient protection of remote access, internet-facing OT, weak password practices, default credentials, inadequate segmentation between IT and OT, weak physical perimeter protection, poor asset inventory, insufficient backup power and cooling, and limited joint training between physical security and cybersecurity teams. The main risk categories and corresponding mitigation strategies are mapped in Table 2.

TABLE 2 MAPPING OF RISK CATEGORIES TO MITIGATION STRATEGIES.

Risk category	Typical risk factors	Recommended strategies
Direct physical attack on infrastructure	Unprotected facilities; limited monitoring; slow response	Perimeter hardening; monitoring; patrols; redundancy
Unauthorized physical access and device compromise	Weak access control; poor asset tracking; removable media	MFA for physical access; visitor control; secure storage; asset inventory
Environmental hazard affecting cyber systems	Fire, flood, heat; power/cooling failure; poor siting	Backup power; environmental sensors; redundant links; DR tests
Compromise of physical-security or OT platforms	Internet-facing devices; default passwords; weak segmentation/logging	Segmentation; remove public exposure; MFA; monitoring; patching
Hybrid cyber-physical scenario	Separate teams; weak exercises; poor information sharing	Joint IR; exercises; alarm correlation; threat intelligence; recovery playbooks

The strategies in Table 2 should be mapped to a governance framework instead of being applied as isolated controls. NIST CSF 2.0 can be used to organize the activities into Govern, Identify, Protect, Detect, Respond and Recover functions [7]. For OT environments, NIST SP 800-82 Rev. 3 emphasizes the need to consider reliability, safety and performance requirements when selecting controls [2]. CISA performance goals also stress prioritized practices for reducing the attack surface and improving resilience in critical infrastructure organizations [8].

The 7SHIELD project illustrates why integrated cyber-physical response is necessary. The project was designed to protect space ground segments against physical, cyber and combined threats and includes prevention, detection,

response and mitigation mechanisms [15]. ENISA also emphasizes security and privacy challenges in IoT-enabled smart manufacturing environments, which are relevant to the protection of industrial cyber-physical systems [16].

The analysis also requires the reclassification of some widely cited cybersecurity incidents. Cases such as ransomware attacks or social-engineering intrusions should not automatically be categorized as physical vulnerabilities. They may be relevant when they disrupt physical services or reveal weaknesses in access-control procedures, but the initial vector must be clearly distinguished from the operational consequence. This distinction improves the precision of incident analysis and addresses the main weakness of broad descriptive approaches.

D. Limitations and Future Research

The study is limited by the availability and detail of public incident information. Many reports do not disclose technical evidence, intrusion paths, physical access conditions, or full impact data. Therefore, the risk scores in Table 1 should be interpreted as structured qualitative assessments, not as verified statistical measurements. Future work should expand the dataset, include interviews with infrastructure operators, compare multiple sectors and test the framework with real organizational risk-assessment data.

Future research should also examine whether cyber-physical incident reporting can be standardized across sectors. Standardized reporting fields - physical vector, cyber/OT asset, operational impact, evidence confidence and recovery time - would allow stronger comparison and trend analysis over time.

CONCLUSIONS

The revised analysis shows that the physical vulnerability of cyber systems is a multi-dimensional problem involving facilities, devices, environmental dependencies, OT assets, access-control systems and incident-response processes. The article therefore distinguishes direct physical compromise from cyber incidents with physical consequences. This distinction is necessary because not every cyberattack that affects an organization is a physical vulnerability, while not every physical event is a cyberattack.

The proposed methodological framework supports a more precise assessment of incidents by verifying the physical component, mapping the affected asset and dependency, applying an ordinal risk score, assigning the incident to an analytical category and selecting mitigation strategies. The incident summary and timeline provide a clearer overview of how different physical and cyber-physical mechanisms affect critical infrastructure and cyber systems.

The main practical implication is that organizations should integrate physical security and cybersecurity governance. Protection should include access control, asset inventory, segmentation, remote-access management, environmental monitoring, independent safety

mechanisms, incident-response exercises and recovery planning. By applying an integrated approach aligned with current OT and cybersecurity frameworks, organizations can reduce exposure, improve resilience and respond more effectively to combined physical and cyber threats.

REFERENCES

- [1] Allied Universal, "World Security Report 2023," 2023. [Online]. Available: https://www.worldsecurityreport.com/media/v1ahrj2v/a4_world-security-report_vf_en.pdf. [Accessed: May 4, 2026].
- [2] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, and S. H. Le, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82 Rev. 3, 2023. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-82r3>. [Accessed: May 4, 2026].
- [3] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. T. Ahmed, "Cyber-physical systems security: A systematic review," *Computers & Industrial Engineering*, vol. 188, 109891, Feb. 2024, <https://doi.org/10.1016/j.cie.2024.109891>.
- [4] A. Akbarzadeh and S. K. Katsikas, "Dependency-based security risk assessment for cyber-physical systems," *International Journal of Information Security*, vol. 22, no. 3, pp. 563-578, 2023, <https://doi.org/10.1007/s10207-022-00608-4>.
- [5] X. Lyu, Y. Ding, and S.-H. Yang, "Safety and security risk assessment in cyber-physical systems," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 221-232, 2019, <https://doi.org/10.1049/iet-cps.2018.5068>.
- [6] N. Agrawal and R. Kumar, "Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey," *ISA Transactions*, vol. 130, pp. 10-24, 2022, <https://doi.org/10.1016/j.isatra.2022.03.018>.
- [7] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, Feb. 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>. [Accessed: May 4, 2026].
- [8] Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," 2023. [Online]. Available: <https://www.cisa.gov/cybersecurity-performance-goals-cpgs>. [Accessed: May 4, 2026].
- [9] National Conference of State Legislatures, "Human-Driven Physical Threats to Energy Infrastructure," May 22, 2023. [Online]. Available: <https://www.ncsl.org/energy/human-driven-physical-threats-to-energy-infrastructure>. [Accessed: May 4, 2026].
- [10] NASA Jet Propulsion Laboratory, "Glass Fire, September 27, 2020," Oct. 7, 2021. [Online]. Available: <https://www.jpl.nasa.gov/images/pia24209-glass-fire-september-27-2020/>. [Accessed: May 4, 2026].
- [11] Verkada, "Verkada Security Update - Incident Report," 2021. [Online]. Available: <https://www.verkada.com/security-update/report/>. [Accessed: May 4, 2026].
- [12] Dark Reading, "Lights Out: Cyberattacks Shut Down Building Automation Systems," 2021. [Online]. Available: <https://www.darkreading.com/cyberattacks-data-breaches/lights-out-cyberattacks-shut-down-building-automation-systems>. [Accessed: May 4, 2026].
- [13] BBC News, "Hacker tries to poison water supply of Florida city," Feb. 8, 2021. [Online]. Available: <https://www.bbc.com/news/world-us-canada-55989843>. [Accessed: May 4, 2026].
- [14] Cyber Threat Intelligence Integration Center, "Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023-April 2024," Office of the Director of National Intelligence, June 2024. [Online]. Available: https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf. [Accessed: May 4, 2026].
- [15] European Commission, CORDIS, "Safety and Security Standards of Space Systems, Ground Segments and Satellite Data Assets, via Prevention, Detection, Response and Mitigation of Physical and Cyber Threats (7SHIELD)," Project Fact Sheet, 2023. [Online]. Available: <https://cordis.europa.eu/project/id/883284>. [Accessed: May 4, 2026].
- [16] ENISA, "Good Practices for Security of Internet of Things in the Context of Smart Manufacturing," 2018. [Online]. Available: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iiot>. [Accessed: May 4, 2026].

A “Brute Force” Reduced Attack Implementation on 256 - AES Encrypted Voice Stream in a MATLAB Simulink Environment

Elitsa Petkova

Directorate "C4I Systems Development"
 Bulgarian Defence Institute
 Sofia, Bulgaria
 ellydpetkova@gmail.com

Abstract — This article presents the steps and the possibility of implementing a reduced “Brute force” attack on a 256-AES encrypted voice stream in a MATLAB Simulink environment. The focus of the study is not on the computational power and the impossibility of performing 2^{256} calculations, but on the selection of the correct decrypted ciphertext from many candidates. The main idea is that decryption is performed based on signal processing, unlike classical cryptanalysis methods. The analog waveform after decryption and decoding carries information whether the corresponding decryption is a function of the "correct" key or not.

Keywords— AES, attack, Brute force, voice stream, cryptanalysis.

I. INTRODUCTION

The AES (Advances Encryption Standard) block cipher was designed in 1997 [1] and is one of the most widely used cryptographic primitives. AES is built on a substitution-permutation network. It encrypts/decrypts blocks of fixed length 128 bits and uses three key lengths, each of which requires a certain number of rounds:

- 128-bit key - 10 rounds;
- 192-bit key - 12 rounds;
- 256-bit key - 14 rounds;

The functionality of the algorithm is presented in Fig. 1 [2] and includes a function for expanding the key according to its length and a series of functions.

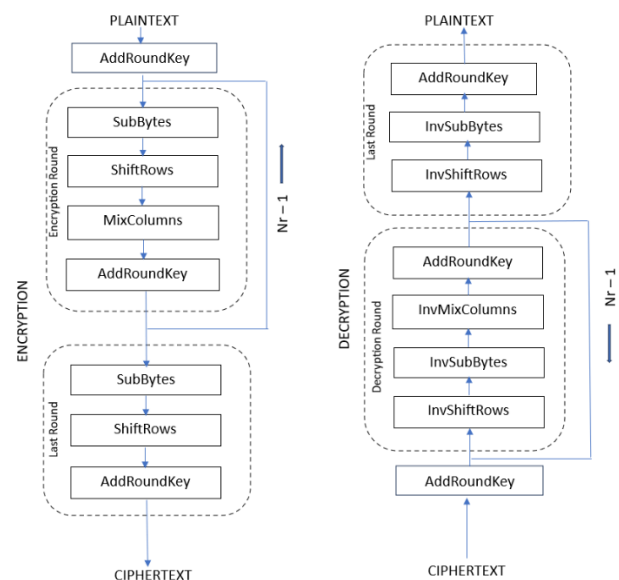


Fig. 1 AES functionality

AES is subject to many cryptanalysis. A popular attempt at cryptanalysis of AES with local collisions is the one applied to the related key model [3]-[6]. It requires not only ciphertexts but also a certain number of corresponding plaintexts, and also has key requirements. From the data complexity perspective, the “Meet in the middle” attack with bicliques, applied to AES [7] is effective, but also has a key requirements. In [8] is presented biclique cryptanalysis of full AES. It also requires ciphertexts and a certain amount of corresponding plaintexts.

From the perspective of the transmitted information, when transmitting voice streams over wireless networks, a potential attacker could only obtain the transmitted ciphertexts.

Therefore, considering the cryptanalysis of voice streams, it can be concluded that the cryptanalytic approaches developed so far, requiring ciphertexts and a certain amount of corresponding plaintexts, are impractical. They only prove certain structural weaknesses in the cipher design. A practical cryptanalytic approach would be one, requires only ciphertexts.

A “Brute force” attack is of no interests to cryptanalysts. Its application requires solving two main problems:

- to provide the necessary computational resources to perform the mathematical calculations;
- to design a method that selects the real decryption from the multitude of such;

To apply a “Brute force” attack on voice streams with 256 bits AES, 2^{256} calculations are required. Now, there is no technology that could provide them. A technological breakthrough and implementation in this direction could be expected in the near future due to the rapid progress of quantum technologies [9] – [11]. On the other hand, the secured computing resource cannot ensure the selection of a real decryption from a multitude of such. In this publication, the focus will be on the implementation and analysis of a method for selecting a real plaintext (decryption) when implementing a “Brute force” attack in a reduced form.

According to the conceptual design, one of the factors for the success of a “Brute force” attack is that it is directly dependent on the output sequences during decryption, determining the form of the analog signal. Fig.2 and Fig. 3 present a conceptual model of encoding, encryption and decryption and decoding of human speech, respectively. The display in Fig.2 visualizes the data before signal processing - encoding and encryption, and the display in Fig.3 - after decoding and decryption. They represent values along the ordinate in the coordinate system. The input data is a function of an audio file that contains a dialogue between two people communicating in Bulgarian. The process of discretization of the signal determines its values along the abscissa. The differences in the values on the two displays, determining the analog signal, are due to the encoding and decoding functions.

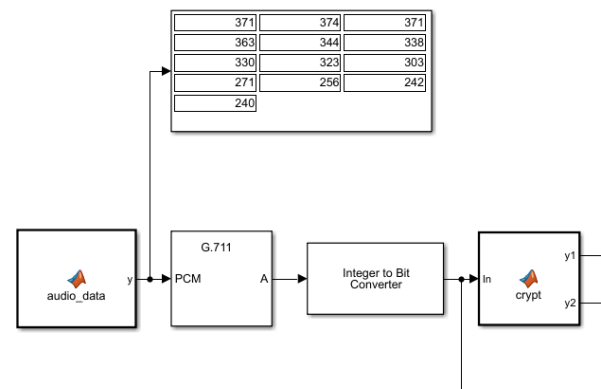


Fig. 2 Conceptual model of encoding and encryption of audio data

The “Verification” block in Fig. 3 performs the corresponding function and outputs a result of “0” if the input data before encryption and after decryption match. Accordingly, it outputs “1” if there is an error in the encryption or decryption module.

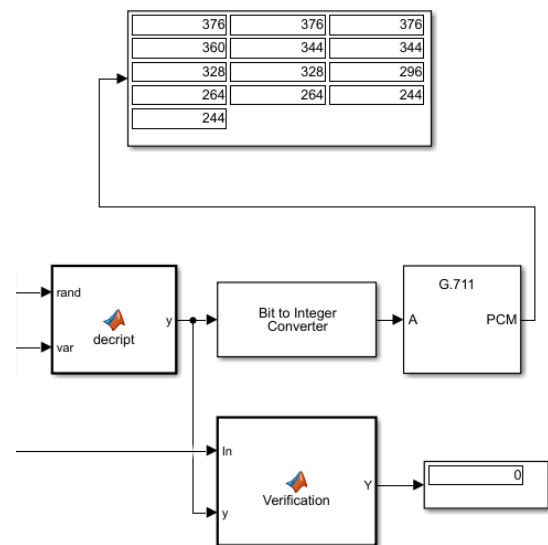


Fig. 3 Conceptual model of decoding and decryption of audio data

This article is structured as follows - in the “TEST SETUP” section, the electrical circuit implementing the reduced “Brute force” attack model in the order of Matlab 2019a – Simulink is described, and in the “EXPERIMENTAL PART”, the results of the experiment are described. In “CONCLUSION”, the conclusions from the non-standard method of applying a reduced “Brute force” attack are described.

II. TEST SETUP

Many implementations of AES [12], [13], [14], [15] have been created on different development environments. They are not suitable for the present study. For the purpose of the present study, the model should be developed in the Matlab Simulink environment.

The “Brute force” attack model is in reduced form. The model is implemented in a Matlab 2019a – Simulink environment. The computer configuration to be used – CPUx4 (8Tread), 2.2 GHz each core, RAM 8GB DDR4, 2400MHz, operating system – Windows 10 Professional.

Fig. 4 presents some of the blocks necessary for the implementation of the attack. The “audio_data” block contains data in the format of integer values generated from a sound file containing human speech. The “G. 711” codec encodes the data in the PCM (Pulse Code Modulation) to A-low format. Encoded data should be converted to binary, this function is performed by the “Integer to Bit Converter” block. In binary format, they are fed to the encrypt block, which encrypts them with 256 bits AES. The software implementation of the encryption function is presented in [16]. The “Rand” block generates IV (Initialization Vector) and keys required for the attack.

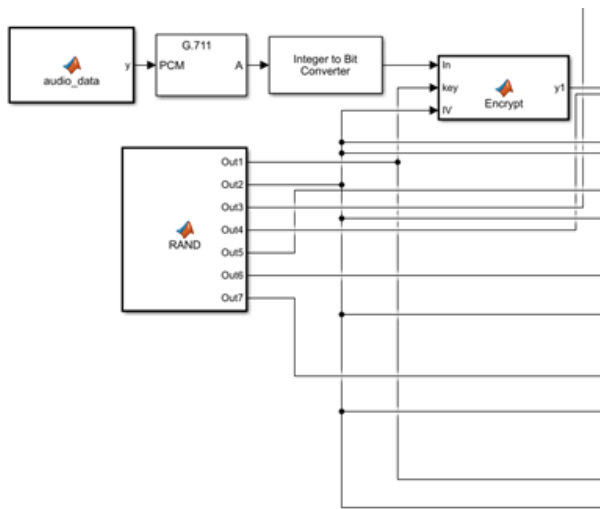


Fig.4 Experimental model of application of Brute Force attack in reduced form, including the blocks – “audio_data”, “G. 711”, “Integer to Bit Converter”, “Rand”, “Encrypt”;

The attack will be mitigated by not using all 2^{256} key combinations in the decryption process, but only six, five of which are random and one is real. The decryption is performed in parallel and is presented in fig. 5.

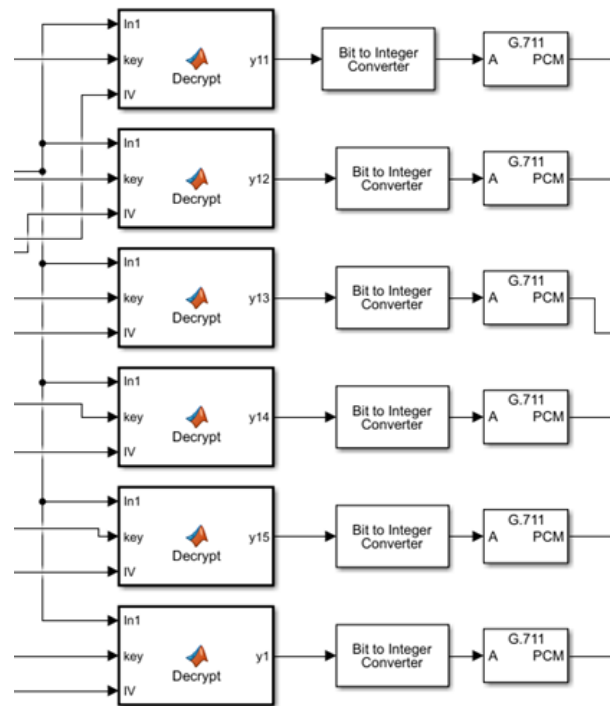


Fig.5 Experimental model of application of Brute Force attack in reduced form, including the blocks – “Decrypt”, “Bit to Converter”, “G. 711”;

The “Bit to Integer Converter” blocks convert the data from binary to integer, after which the “G. 711” codecs decode them, after which they should be sent to the selection block. The result is visualized on a display. They are presented in fig. 6.



Fig. 6 Experimental model of application of “Brute force” attack in reduced form, including the “select_data” block and display;

III. EXPERIMENTAL PART

An AES encryption consists of 128 bits, equal to 16 integer values. The focus of the conceptual design is that the input sequence, before encoding and encryption, and the output sequence, after decryption and decoding, represent sixteen analog values along the ordinate in the coordinate system.

Since they are a function of human speech, they change smoothly. When decrypted with the wrong key, a sequence of randomly changing integer values is obtained, shown in Fig. 7. This property is the basis for implementing a method for selecting a decrypted sequence with the correct key.

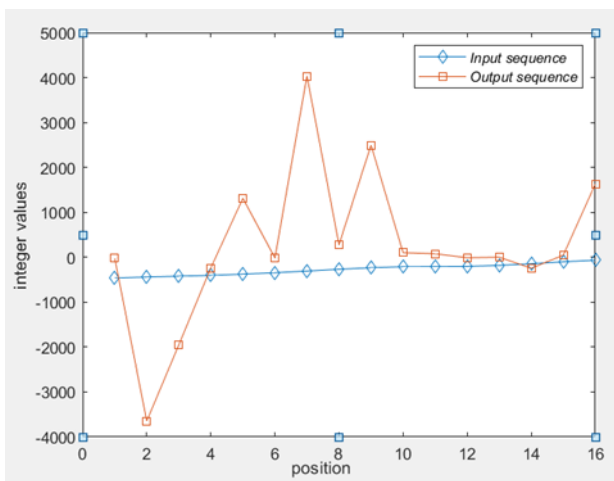


Fig. 7 Input sequence and output decrypted with the wrong key

The focus when creating a selection algorithm is to look for dependencies in the output sequences when decrypting with a "correct" key, which are absent when decrypting with a "wrong" one. This is done by searching for the distance between each two adjacent values. When decrypting with a “correct” key, this distance has certain limitations. The selection algorithm is logically connected to a verification method. Their development should be described in a separate publication.

After conducting multiple experiments with different input values and key sequences, it can be concluded that the block performs the function of selecting the correct decryption.

Fig. 8 visualizes the one input and correctly decrypted output sequence.

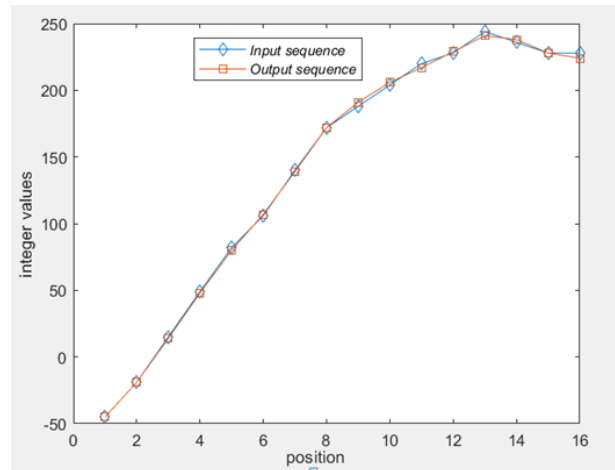


Fig.8 Input and correctly selected output sequence

One of the results of the conducted experimental studies, visualizing all six decryptions, is shown in Fig. 9.

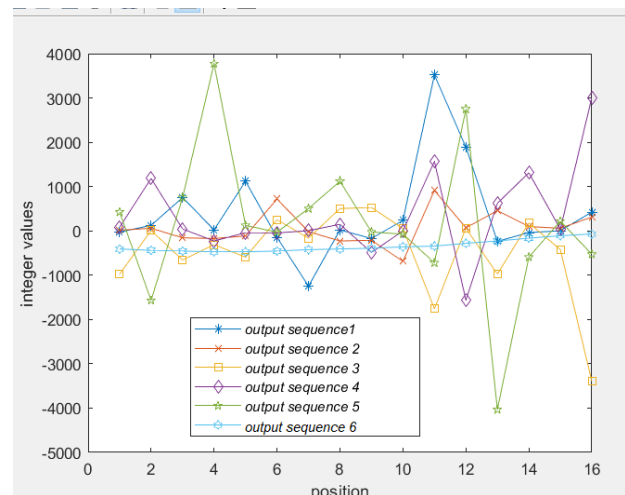


Fig.9 Decrypted output sequences

IV. CONCLUSION

A method for reduced form a “Brute force” attack in Matlab 2019a – Simulink environment has been developed. A selecting method the correct decryption from the set of such has been developed. The method is not based on standard cryptanalytic approaches, but on signal processing. The method has been experimentally studied. The next step in this research is to develop a method for verification of the selected sequence.

REFERENCES

- [1] J. Daemen, V. Rijmen, “The Design of Rijndael: AES - The Advanced Encryption Standard”, Springer, 2002, Available: <https://link.springer.com/book/10.1007/978-3-662-04722-4> [Accessed April 27, 2026]

- [2] R. Ganesh, B. Khan, A. Khan, A. Kasin, "A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real – world applications, and post – quantum challenges", *International Journal of Information*, vol. 24, no 216 (2025), Available: <https://link.springer.com/article/10.1007/s10207-025-01116-x> [Accessed June 9, 2026], <https://doi.org/10.1007/s10207-025-01116-x>
- [3] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, "Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds", In *EUROCRYPT'10*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 299–319. Springer, 2010.
- [4] A. Biryukov, D. Khovratovich, "Related-Key Cryptanalysis of the Full AES-192 and AES-256", In *ASIACRYPT'09*, vol. 5912 of *Lecture Notes in Computer Science*, pp. 1–18. Springer, 2009.
- [5] A. Biryukov, D. Khovratovich, I. Nikolić, "Distinguisher and related-key attack on the full AES-256", In *CRYPTO'09*, vol. 5677 of *Lecture Notes in Computer Science*, pp. 231–249. Springer, 2009
- [6] A. Biryukov, I. Nikolić, "Automatic Search for Related-Key Differential Characteristics in Byte - Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others", In *EUROCRYPT'10*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 322–344. Springer, 2010.
- [7] Orr Dunkelman and Nathan Keller. "The effects of the omission of last round's MixColumns on AES", *Inf. Process. Lett.*, 110(8-9), pp. 304–308, 2010, Available: <https://eprint.iacr.org/2010/041.pdf> [Accessed April 27, 2026]
- [8] A. Bogdanov, D. Khovratovich, Ch. Rechberger, "Biclique Cryptanalysis of the Full AES", *Lecture Notes in Computer Science*, pp. 344–371. Springer, 2011, Available: https://www.researchgate.net/publication/221326929_Biclique_Cryptanalysis_of_the_Full_AES [Accessed April 27, 2026]
- [9] L. Grover, "From Schrödinger's equation to the quantum search algorithm", *American Journal of Physics* pp. 769-777, 2001. Available: <https://arxiv.org/pdf/quant-ph/0109116>, [Accessed June 8, 2026]
- [10] C. H. Bennett, E. Bernstein, G. Brassard, U. Varirani, "The strength and weaknesses of quantum computation". *SIAM Journal on Computing*, 26(5), pp. 1510-1523, 1996. Available: <https://arxiv.org/pdf/quant-ph/9701001>, [Accessed June 8, 2026]
- [11] S. Rao, D. Mahto, D. Yadav, Danish, D. Khan., "The AES-256 Cryptosystem Resist Quantum Attacks", *International Journal of Advanced Research in Computer Science*, 2017, 8(3) p. 404-408 Available: https://www.researchgate.net/publication/316284124_The_AES-256_Cryptosystem_Resists_Quantum_Attacks, [Accessed June 8, 2026]
- [12] R. Andriani, S. Wijayanti, F Wibowo, "Comparision of AES 128, 192 and 256 Bit Algorithm For Encryption and Decryption File", 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2018.
- [13] M. Muzakkir, M. Nadzri, A. Ahmad, A. Amira, "Implementation of Advanced Encryption Standard (AES) for Wireless Image Transmission using LabVIEW", *IEEE 16th Student Conference on Research and Development (SCoRED)*, Bangi, Malaysia, 2018.
- [14] Ch. Su, T. Lin, Ch. Huang, Ch. Wu, "A High – Throughput Low – Cost AES Processor" *IEEE Communications Magazine*, vol. 41, p. 86-91, Available: <https://ieeexplore.ieee.org/document/1252803>, <http://www.umi.com/proquest/> [Accessed June 9, 2026], <https://doi.org/10.1109/MCOM.2003.1252803>
- [15] A. Kumar, N. Tiwar, "Effective Implementation and Avalanche Effect of AES", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, vol. 1, no. 3/4, p. 31-35 Available: https://www.researchgate.net/publication/267802536_Effective_Implementation_and_Avalanche_Effect_of_AES, [Accessed June 9, 2026]
- [16] E. Petkova, M. Angelov, „Implementation of “Advanced Encryption Standard” in the Matlab – Simulink environment“ Scientific conference “Current security problems”. October 9-10, 2025, Veliko Tarnovo, Bulgaria , 2025

Verifying Aspects an "Brute Force" Attack on 256 - AES Encrypted Voice Stream

Elitsa Petkova

Directorate "C4I Systems Development"
Bulgarian Defence Institute
Sofia, Bulgaria
ellydpetkova@gmail.com

Mario Angelov

Directorate "C4I Systems Development"
Bulgarian Defence Institute
Sofia, Bulgaria
m.angelov@di.mod.bg

Abstract — The rapid development of quantum technologies leads to new possibilities applying certain cryptographic attacks against symmetric algorithms. This paper discusses a verifying method an different approach to applying an "Brute force" attack on 256 - AES encrypted voice stream. Verification is performed after the correct decryption is selected from the set of decryptions. The purpose of verification is that if the selection module has accepted an incorrect decryption as correct, then the error is registered during verification. Unlike the classic application of a "Brute force" attack, which emphasizes computing power, here the focus is on signal processing.

Keywords — AES, attacks, Brute force, voice streams, cryptanalysis.

I. INTRODUCTION

AES is a stream cipher approved by NIST [1]. The classic scenario for applying a "Brute force" attack on encrypted data with 256 – AES requires 2^{256} calculations. Providing a computational resource that provides the necessary calculations is only one of the tasks that need to be performed for the attack to be practical. The other significant problem is selecting the correct decryption from the set of such. From the point of view of transmitting encrypted voice streams in wireless networks, there is a practical approach for applying a "Brute force" attack, applied in a reduced form, developed in the Matlab 2019a – Simulink environment. It should be published. At present, there is no developed cryptanalytic approach, except for "Brute force", requiring only ciphertext. The developer of the "Twofish" algorithm - one of the most popular world-renowned cryptographers - Bruce Schneier, [2] claims that it is impossible to construct an attack that will lead to the deciphering of traffic. The attacks developed so far represent "academic cracking of the cipher". In fact, from the point of view of voice streams transmitted over a wireless network, a practical and feasible attack would be the one that requires only the ciphertext.

AES is resistant to classical differential cryptanalysis, but is susceptible to related key attacks. The published cryptanalysis methods applied to the AES block cipher require both ciphertext and a certain number of corresponding plaintexts, and also have requirements for the key [3-10]. A variant of differential cryptanalysis is presented in [11], in which the cipher is split into two parts, each part computed with partial knowledge of the key. In the middle, the attacker computes guesses for the key, checking for matches. A different but original attack is presented in [12]. It operates on the principle of inducing random errors in the cipher state matrix. The induction leads to defective ciphertexts, which allows the full key to be deduced. From a practical point of view, a "Brute force" attack would be real and practical, since it only requires ciphertext. The disadvantage in this case is the need for computational resources, which depends on the development of technologies.

There are two typical ways of applying a "Brute force" attack on voice stream::

- classical - if we have a speech stream consisting of " n " consecutive encryptions, it follows that decrypted messages must be listened to, from which the correct one can be chosen. If we denote the listening time for one encryption by " t_n " then the listening time for the entire message would be $t_{full} = n \cdot 2^{256}$. This requirement makes it impossible to implement the attack in the classical scenario.
- by selection and subsequent verification – method presented in this publication. The main idea is to perform selection not on the entire encrypted voice message, but only on one encryption - 128 bits. The goal is to save both computational and time resources. Similarly, verification will also require one

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.223>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

encryption. If the first attempt at selection and verification generates a result, then the execution time of the attack will be $t_{perf} = t_{sel} + t_{ver}$, where t_{sel} denotes the time required for selection, and t_{ver} denotes the time required for verification. If " m " attempts are required to generate a result, then the time required for the attack will be $t_{full} = m \cdot t_{perf}$. This attack variant is fully feasible if there is a technology that can perform 2^{256} calculations.

This article is structured as follows - in the section "functional model" the methodology for selection and subsequent verification is discussed, in the module "experimental part" some special cases of possible wrongly selected sequences are discussed, which confirm the need for verification. The module "results" gives a generalized assessment of the experiments performed, and in the "conclusion" the motives for conducting the present study are discussed.

II. FUNCTIONAL MODEL

In order to design a properly functioning selection algorithm, multiple decryptions of voice streams have been considered and analyzed. Within a decryption consisting of 16 integer values corresponding to 128 bits, we mark a given current integer value with " n " and the next one with " $n + 1$ ". Then the distance between them - Δ_n represents the sum or difference or absolute value of the difference of two adjacent values or of their absolute value.

As a result of experimental data analysis, the highest value of Δ_n in decryptions with a "wrong" key is $\Delta_n = 7808$, while in those with a correct key it is of $\Delta_n = 1170$, encountered once in a single decryption. If we set an upper bound for delta Δ_n , we can implement an algorithm based on the following postulate - if for a given decrypted sequence consisting of sixty integer values, there is more than one $1300 > \Delta_n \geq 1200$, then the corresponding sequence was not decrypted with a correct key. Experimental results for calculating all Δ_n values when applying a reduced "Brute force" attack for one encryption and six parallel decryptions are presented in Table 1. A reduced "Brute force" attack involves six parallel decryptions, the first five decrypted with a pseudo-random key, the sixth decryption with a real key.

The principle of operation of the verification module is the same as the selection module. If the selection module misses an incorrect decryption, the probability of the same thing happening during verification - another sequence decrypted with the same key - is negligible. Both modules are executed using the following program code:

```

provX = 0;
for i = 1:15
    if (InX(i+1)<=0 && InX(i) >=0)
        minX(i) = abs(InX(i+1)) +
InX(i);
        if minX(i) > 1300
            provX = 2;
        end
        if minX(i) >= 1200
            provX = provX + 1;
        end
    elseif (InX(i+1)>=0 && InX(i)
<=0)
        minX(i) = InX(i+1) +
abs(InX(i));
        if minX(i) > 1300
            provX = 2;
        end
        if minX(i) >= 1200
            provX = provX + 1;
        end
    elseif (InX(i+1)<=0 && InX(i)
<=0)
        minX(i) = abs(abs(InX(i+1))
- abs(InX(i)));
        if minX(i) > 1300
            provX = 2;
        end
        if minX(i) >= 1200
            provX = provX + 1;
        end
    elseif (InX(i+1)>=0 && InX(i)
>=0)
        minX(i) = abs(InX(i+1) -
InX(i));
        if minX(i) > 1300
            provX = 2;
        end
        if minX(i) >= 1200
            provX = provX + 1;
        end
    end
end
if provX <= 1
    Out1 = Out(X:X+15,1);
else
    Out1 =
int16([0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0
]);
end

```

Software implementation of the selection method

TABLE 1 REDUCED “BRUTE FORCE” ATTACK FOR ONE KRANDOM ENCRYPTION

Output sequence	Δ_1	Δ_2	Δ_3	Δ_4	Δ_5	Δ_6	Δ_7	Δ_8	Δ_9	Δ_{10}	Δ_{11}	Δ_{12}	Δ_{13}	Δ_{14}	Δ_{15}
1	30	3579	5408	1875	74	127	1636	416	2350	274	1468	1643	10	131	1252
2	1726	1726	3456	3648	2110	3102	2983	38	68	34	93	546	880	503	281
3	1299	1263	107	208	2026	2157	12	3845	3877	75	51	26	245	368	900
4	1109	29	65	53	3322	2384	1033	227	220	447	1991	1656	1208	3200	1812
5	1558	1196	146	230	580	180	43	191	756	714	42	86	394	128	408
6	0	24	30	28	23	14	36	38	45	32	26	32	24	32	24

The algorithm of the “Brute force” attack functionality, including selection and verification blocks, is presented below in fig. 1. There is a counter with a zero initial value, which increases the value by one upon selection. After selecting a potential decrypted sequence, a verification process follows. If the potential sequence turns out to be real, the result is visualized on a display, otherwise the counter is reset and the attempts continue.

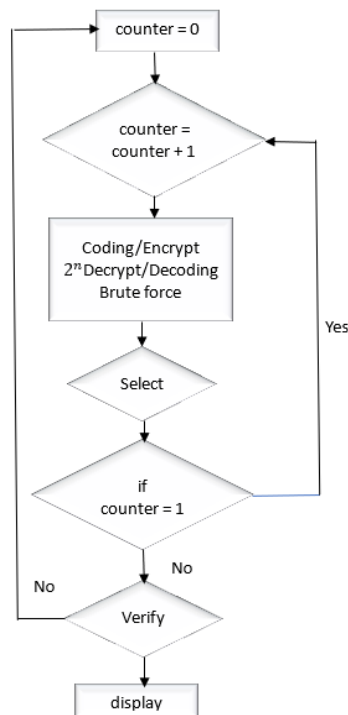


Fig. 1. Functional model of application of brute force attack with selection and subsequent data verification

III. EXPERIMENTAL PART

A “Brute force” attack is implemented in a reduced form in a Matlab 2019a – Simulink environment and should be published. The input sequence is a voice stream in the form of integer values. The output sequence after the overall signal processing also represents integer values

close to or equal to the input. The small differences are due to the encoding and decoding processes.

The principle of operation of the verification module is the same as the selection module. The selection module is designed so that there is a possibility that it will select a sequence decrypted with the wrong key, i.e. it is possible to make an error. The assumption is that if decryption with an incorrect key produces an integer result that passes the selection module successfully, then the probability of this happening again when decrypting the next 128-bit sequence with the same key during verification is negligible. The model is designed so that the module only generates a result if the result is verified. The purpose of the experiment is to assess the effectiveness of the selection process and the need for a verification process.

We will look at several scenarios that confirm the need for verification

Hypothesis 1 – We perform a process of encryption and decryption of a given 128 bits sequence with the same key. The input and output sequences match. After the decryption process, we invert the least significant bit of the sequence in order to simulate a random result of applying a “Brute force” attack, similar to the real one. Fig. 2 shows a graph of the input and modified output sequence. It successfully passes the selection module.

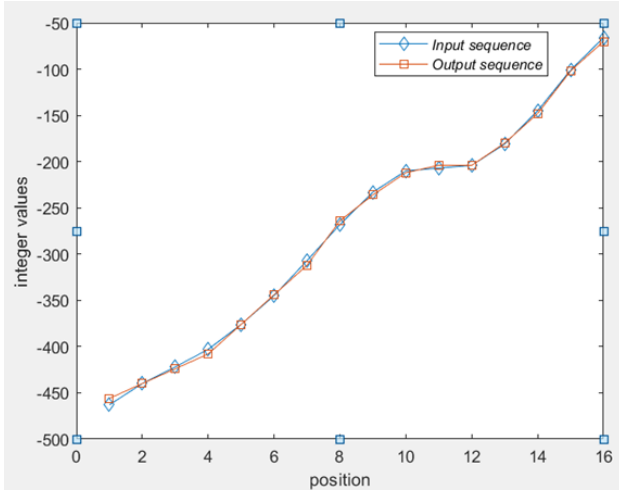


Fig. 2 Input and selected output sequence according to hypothesis 1

Hypothesis 2 – we repeat the scenario as for each integer value out of a total of 16 such for an encryption corresponding to 128 bits, we invert the least significant bit. The implementation of the hypothesis is presented with the following algorithm in the form of program code:

```
nn = 8;
while nn <= 128
    y1(nn, 1) = ~y1(nn, 1);
    nn = nn + 8;
end
```

Software implementation of a hypothesis 2

Fig. 3 presents a graph of the input and modified output sequence. Analogous to hypothesis 1, despite the difference in the number of inverted bits, the output sequence successfully passes through the selection module.

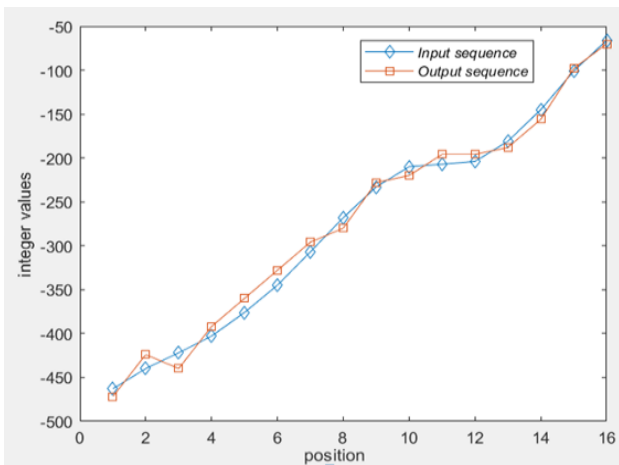


Fig. 3 Input and selected output sequence according to hypothesis 2

Hypothesis 3 – for each integer value out of a total of 16 such for an encryption corresponding to 128 bits, we

invert the most significant bit. The result is presented in Fig. 4

The huge difference in the values between the input and the selected output sequence is due to the G.711 codec. In the experimental model, it performs the functions of encoding and decoding. In it, the most significant bit of a given binary equivalent of an integer value is determined by the sign in front of the value. In this case, all the most significant bits of the entire binary sequence are inverted. The input and output sequences are mirrored with respect to the "X" axis. The output sequence passes successfully through the selection module.

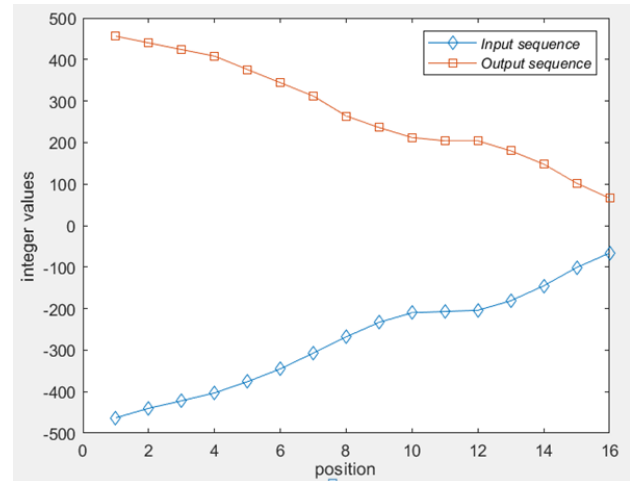


Fig. 4 Input and selected output sequence according to hypothesis 2

It is impossible to predict which of all 2^{256} the key options when applying a brute force attack would generate output sequences, according to the scenarios described above and many others. Fig. 5 only visualizes what two consecutive sequences would look like - the first selected and the second rejected during verification. It is visible that the first 16 values change smoothly, which is why they successfully pass through the selection module. It is visible that the first 16 values change smoothly, which is why they successfully pass the selection module. The second 16 values are chaotic. They should not be allowed to pass during verification.

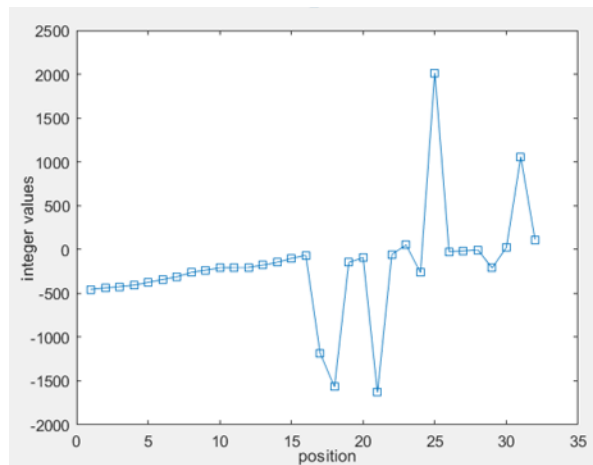


Fig. 5 Potential selected and rejected sequences during verification

IV. RESULTS

The experiments were conducted with the same input sequence and the same key. Since the number of possible decryptions in the MATLAB 2019a – Simulink environment is very limited, the conducted experiment aims to evaluate the effectiveness of the selection module and the need for a verification module. The results show that a certain number of sequences pass through the selection module, which, in the format of integer values, are sequential, not chaotic. With a limited number of experiments, the verification module works effectively.

V. CONCLUSION

This article presents certain aspects of designing selection and verification modules for applying a reduced brute force attack on voice streams. This need arises from the fact that the classical application of the attack does not carry information about which is the correct decryption from the set of such. The interest in “Brute force” attack stems from the fact that it does not depend on the mathematical construction of the algorithm, but only on the length of the key and the availability of computational resources. Technological progress in quantum technologies leads to the fact that compared to symmetric algorithms including AES, Grover's algorithm [13],[14] increases the probability of effective application of brute force attack. It provides quadratic acceleration [15], therefore, with 256 - AES it would require $O(2^{128})$ attempts to implement the attack, comparable to $O(2^{256})$ attempts applied on a classical computer system. Despite technological progress, at the moment 256-bit AES remains computationally unbreakable. It is a matter of the near future for this to happen.

REFERENCES

- [1] J. Daemen, V. Rijmen, “The Design of Rijndael: AES - The Advanced Encryption Standard”, Springer, 2002, Available: <https://link.springer.com/book/10.1007/978-3-662-04722-4> [Accessed April 27, 2026]
- [2] B. Schneier, “Schneier on Security”. [Online]. Available: <https://www.schneier.com/crypto-gram/archives/2000/1015.html> [Accessed June 8, 2026]
- [3] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, “Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds”, In EUROCRYPT’10, vol. 6110 of Lecture Notes in Computer Science, pp. 299–319. Springer, 2010.
- [4] A. Biryukov, D. Khovratovich, “Related-Key Cryptanalysis of the Full AES-192 and AES-256”, In ASIACRYPT’09, vol. 5912 of Lecture Notes in Computer Science, pp. 1–18. Springer, 2009.
- [5] A. Biryukov, D. Khovratovich, I. Nikolić, “Distinguisher and related-key attack on the full AES-256”, In CRYPTO’09, vol. 5677 of Lecture Notes in Computer Science, pp. 231–249. Springer, 2009.
- [6] A. Biryukov, I. Nikolić, “Automatic Search for Related-Key Differential Characteristics in Byte - Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others”, In EUROCRYPT’10, vol. 6110 of Lecture Notes in Computer Science, pp. 322–344. Springer, 2010.
- [7] A. Bogdanov, D. Khovratovich, Ch. Rechberger, “Biclique Cryptanalysis of the Full AES”, Lecture Notes in Computer Science, pp. 344–371. Springer, 2011, Available: https://www.researchgate.net/publication/221326929_Biclique_Cryptanalysis_of_the_Full_AES [Accessed April 27, 2026]
- [8] Ch. Boura, P. Derbez, M. Funk, “Related – Key Differential Analysis of the AES”, IACR Transactions on Symmetric Cryptology, vol. 2023, no. 4, pp. 215 – 243, Available: <https://tosc.iacr.org/index.php/ToSC/article/view/11286/10818> [Accessed June 8, 2026], <https://doi.org/10.46586/tosc.v2023.i4.215-243>
- [9] B. Tao, H. Wu, “Improving the Biclique Cryptanalysis of AES”, Information Security and Privacy. Lecture Notes in Computer Science, vol. 9144, pp. 39- 56, Springer, Available: https://link.springer.com/chapter/10.1007/978-3-319-19962-7_3 [Accessed June 8, 2026]
- [10] A. Bogdanov, D. Chang, M. Ghosh., S.K. Sanadhya, “Bicliques with minimal data and time complexity for AES” In: Lee, J., Kim, J. (eds.) Information Security and Cryptology-ICISC 2014. Lecture Notes in Computer Science, pp. 160–174. Springer, 2014
- [11] Ch. Boura, N. David, P. Derbez, G. Leander, M. Naya-Plasencia “Differential meet-in-the-middle cryptanalysis”, In CRYPTO 2023, Part III, vol. 14083 of Lecture Notes in Computer Science, pp. 240–272. Springer, 2023.
- [12] Dh. Saha, D. Mukhopadhyay, D. Roy Chowdhury. "A Diagonal Fault Attack on the Advanced Encryption Standard", Available: <https://eprint.iacr.org/2009/581.pdf>, [Accessed June 8, 2026]
- [13] L. Grover, "From Schrödinger's equation to the quantum search algorithm", American Journal of Physics pp. 769-777, 2001. Available: <https://arxiv.org/pdf/quant-ph/0109116>, [Accessed June 8, 2026]
- [14] C. H. Bennett, E. Bernstein, G. Brassard, U. Varirani, “The strength and weaknesses of quantum computation”. SIAM Journal on Computing, 26(5), pp. 1510-1523, 1996. Available: <https://arxiv.org/pdf/quant-ph/9701001>, [Accessed June 8, 2026]
- [15] S. Rao, D. Mahto, D. Yadav, Danish, D. Khan., “The AES-256 Cryptosystem Resist Quantum Attacks”, International Journal of Advanced Research in Computer Science, 2017, 8(3) p. 404-408 Available: https://www.researchgate.net/publication/316284124_The_AES-256_Cryptosystem_Resists_Quantum_Attacks, [Accessed June 8, 2026]

Compact Critical Infrastructure Active Drone Protection System – Conceptual Design

Zhivo Petrov

Defense Advanced Research Institute
Rakovski National Defense College
Sofia, Bulgaria
ORCID: [0000-0003-2757-0030](https://orcid.org/0000-0003-2757-0030)

Lyubosvet Stoev

Defense Advanced Research Institute
Rakovski National Defense College
Sofia, Bulgaria
ORCID: [0000-0002-2014-4402](https://orcid.org/0000-0002-2014-4402)

Abstract—*The ever growing threat of hostile and unauthorized drones drives the need for counter-action, starting with early detection and reaction. The low cost and availability of small and low flying drones increases both their extensive use in warfare and the accidents with them in civilian settings. Efficient and adequate counteraction requires a detailed study of the threat and a retrospective analysis of potential solutions to the problem.*

Keywords—*Counter-UAS, drone defense, early warning, radar, electronic warfare, acoustic sensing*

I. INTRODUCTION

The use of unmanned or remotely guided aerial threats is not a new phenomenon. As early as World War II, Germany employed the V-1 flying bomb, a precursor to today's cruise missiles and long-range UAVs. Since then, advances in electronics, communications, and navigation have led to the widespread availability of small and highly capable drones. These systems are now used by state and non-state actors alike for reconnaissance, strike, and harassment missions.

The defense against such aerial threats [1] has evolved from visually guided anti-aircraft fire to highly automated, networked systems integrating multiple sensors and effectors. This article reviews that evolution, focusing on early warning and detection, followed by defensive and neutralization methods, and concluding with an analytical synthesis presented in a historical timeline.

A. Detection and Early Warning

Early warning is the foundation of any effective air and drone defense system. [2] The ability to detect, classify, and track aerial threats in sufficient time enables appropriate engagement decisions and efficient allocation of defensive resources.

The first systematic early warning systems emerged prior to and during World War II. Visual observation posts and acoustic sound locators were initially used to detect incoming aircraft. These methods were limited by weather, human perception, and reaction time. The introduction of radar, most notably the British Chain Home system,

revolutionized air defense by providing long-range detection and centralized command and control.

Flying bombs such as the V-1 highlighted the challenge of detecting small, fast, and low-altitude targets, a problem that remains relevant in modern drone defense.

Visual detection remains a basic but important layer of early warning, particularly at short ranges. Modern systems augment human observers with electro-optical (EO) and infrared (IR) cameras. These sensors provide high-resolution imagery and thermal contrast, enabling detection and identification of drones against complex backgrounds. Automated image processing and artificial intelligence increasingly support these systems by reducing operator workload and false alarms.

Acoustic detection systems use microphone arrays to capture and analyze the characteristic sound signatures of drone propulsion systems. Such systems can be effective against small, low-flying UAVs that are difficult to detect by radar. However, their performance is sensitive to environmental noise, wind, and terrain, making them most effective as part of a multi-sensor architecture rather than as standalone solutions.

Radar remains the primary long-range detection method for aerial threats. Traditional air defense radars were optimized for large, fast aircraft and missiles, but modern drone threats require high-resolution radars capable of detecting small radar cross-section targets flying at low altitude. Specialized counter-UAS radars have been developed to address these challenges, often operating in X-band or Ku-band and employing advanced signal processing techniques.

Many drones rely on radio frequency (RF) links for command, control, and telemetry. Passive RF detection systems monitor the electromagnetic spectrum to identify known drone communication protocols and locate both the UAV and its operator. These systems are valuable because they do not emit energy and can detect drones even when radar signatures are weak.

No single detection modality is sufficient under all conditions. Modern early warning systems therefore rely

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.81>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

on sensor fusion, combining radar, RF, EO/IR, and acoustic inputs into a unified situational picture. [4] Advances in data processing, networking, and artificial

B. Defense and Neutralization Methods

Once a drone is detected and classified as hostile, a range of defensive options is available. These can be broadly divided into kinetic and non-kinetic methods.

Historically, fighter aircraft were the primary means of intercepting aerial threats, including flying bombs and reconnaissance aircraft. Surface-to-air missiles (SAMs) later complemented and partially replaced fighter interception, offering rapid reaction and high engagement probability against high-value targets. While effective against large UAVs, these methods are often impractical or uneconomical against small, low-cost drones. Moreso, they are unaplicable in populated areas – both urban and rural – because of high risk of collateral civilian damage.

Anti-aircraft artillery (AAA) have long been used against low-altitude threats. Modern short-range air defense systems integrate rapid-fire cannons and missile launchers with radar and electro-optical fire control, enabling effective engagement of small UAVs. Proximity-fused ammunition and programmable airburst rounds further enhance effectiveness.

Directed energy weapons, including high-energy lasers and high-power microwave systems, represent an emerging class of counter-UAS effectors. Lasers offer precise, speed-of-light engagement with low cost per shot, while microwave systems can disable drone electronics over a wider area. These technologies are increasingly deployed as part of layered defense systems.

An emerging approach involves using drones to counter drones. Interceptor UAVs can pursue and physically disable hostile drones using nets or kinetic impact. Such systems are particularly suited for urban or civilian environments where collateral damage must be minimized.

C. Historical Analysis and Timeline

The evolution of early warning and defense against drones reflects broader trends in air defense: increasing automation, sensor integration, and a shift from purely kinetic solutions to flexible, multi-layered systems. Table 1 summarizes key developments over time.

TABLE I. TIMELINE OF EARLY WARNING AND DEFENSE AGAINST AERIAL AND DRONE THREATS

Era	Early Warning and Detection	Defense Against Aerial and Drone Threats
1930s – 1940s	visual observers, acoustic sensors, early radar	fighter interception, anti-aircraft guns
1980s–1990s	improved radar resolution, early UAV tracking	SAM modernization, limited EW
2000s	RF detection, early sensor fusion	MANPADS, basic jamming
2010s	multi-sensor systems, EO/IR integration	Dedicated C-UAS systems, EW, nets
2020s	AI-enabled fusion, passive RF and acoustic arrays	lasers, high-power microwaves (HPM),

intelligence have significantly improved classification accuracy and response times, forming the backbone of contemporary counter-UAS architectures.

Era	Early Warning and Detection	Defense Against Aerial and Drone Threats
1930s – 1940s	visual observers, acoustic sensors, early radar	fighter interception, anti-aircraft guns
		interceptor drones

The history of air defense demonstrates that technological change in offensive systems inevitably drives defensive innovation. From the V-1 flying bombs of World War II to today's small, low-cost, and autonomous drones, defenders have repeatedly adapted detection and engagement methods to address new threats. For modern armed forces, counter-UAS is no longer a niche capability but a core element of air defense and force protection. The key lesson is the importance of layered defense: early warning through multiple sensors, rapid decision-making, and the flexible use of kinetic and non-kinetic effectors. As drone technology continues to advance, particularly in autonomy and swarm tactics, successful defense will increasingly depend on integration, automation, and well-trained personnel who understand both the technology and its operational employment.

II. CONCEPTUAL DESIGN OF AN ANTI-DRONE SYSTEM

Based on previous developments [5,6], we suggest a conceptual design of an integrated anti drone system for a typical critical infrastructure site – a controlled area with fixed size. Let us suppose it is a data center, satellite communication relay or a thermal powerplant. For the study, we have fixed the size limiting it to a radius of 1.5 km. Thus the physical layout of the system, as shown on Fig. 1, is:

- Radius: maximum footprint of 1.5 km (all key components within this range).
- Central Command Node (CCN): Buried or hardened structure at the center, hosting the AI-driven fusion & command system.
- Sensor/Effector Layers: Deployed in concentric rings, with overlap and redundancy.

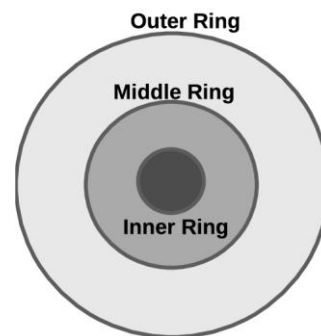


Fig. 1. Sensor Grid Structure.

A. Sensor Grid

Our goal is a 360° multi-elevation coverage with both passive & active sensors and all-weather capacity.

The outer ring is intended for primary early warning. It consists of three parts:

First is an acoustic sensor array: ground mounted microphones to triangulate propeller and engine noise. It works in all weather, though its range would be affected by the wind and the humidity.

The second are the RF (electronic support measures, ESM) Sensors. They detect drone control and telemetry signals and also provide direction finding to identify both drone and operator location. They will work in all conditions.

The third component is a low-power bistatic radar with multiple receivers along the perimeter and one or two transmitters in the middle

The middle ring is at 0.8 km radius. It consists of two layers:

Multi-Function Active Electronically Scanned Array (AESA) Radar. It is the main tracking radar. It consists of multiple small panels on towers/buildings for 360° coverage. This radar is capable of weather filtering (rain/snow clutter suppression).

Electro-Optical/Infrared (EO/IR) Pan-Tilt-Zoom (PTZ) Turrets. They mount high-resolution day cameras and thermal imagers on elevated masts. Thermal vision is effective in fog/light rain but degrades in heavy rain/snow. It is used for visual confirmation and tracking.

The inner ring (>0.3 km) encompasses the critical asset itself. It includes a close-in motion sensors and LIDAR on rooftops. The LiDAR provides high-precision 3D tracking in clear conditions, though is severely degraded in fog/rain. Also, optional are close quarter unauthorized RF, WiFi and Bluetooth signals.

The command post is centered around Sensor Fusion AI ("Sentinel Core"). Its task is to fuse all sensor inputs in real-time, creates a single, confident track. It also should use weather data (both on-site station and external) to weight sensor reliability dynamically (e.g., to rely more on radar and less on EO/IR in fog).

B. Countermeasure Effector Matrix

Our goal is to achieve a scalable effector response from soft kill (and forensic study) to hard kill with absolute minimum collateral damage.

First effector layer is non-kinetic soft kill. It is priority in collateral damage sensitive zones like urban area and close proximity to airports. It includes:

- Spoofers/GPS Simulators. They can take control of or misguide GPS-dependent drones.
- Directional RF Jammers. Located at the middle ring, they employ focused beams to disrupt control, GPS, and telemetry links.

Their power level is adjustable to minimize area effect (crucial in urban settings).

Second layer is hard-kill and includes kinetic and directed energy (DE) effectors.

- High-Power Microwave (HPM) Emitters. Mounted on quick-swivel platforms at the inner ring perimeter. They cause area effect to fry electronics of drone swarms, working line-of-sight, in all-weather.
- Laser Defense Pods (30-50 kW). On stabilized towers, they are silent, low-cost-per-shot and precise. Effective against single drones, though their performance degrades in heavy fog, rain, or snow (high atmospheric attenuation).
- Interceptor Drone "Nests" take the form of 4-6 vertical launch tubes sheltering high-speed quadcopters or fixed-wing interceptors. Equipped with nets, blades and relying on kinetic impact collision capability. They are launched autonomously for beyond-visual-line-of-sight (BVLOS) engagements, especially useful in complex terrain (urban canyons) or against maneuvering targets.
- MANPADS are not integrated into a closed loop. They are held in armory to be used by trained operators under strict rules of engagement against larger high-risk threats.

C. Command and Control (C2) unit

It sits in a central hardened location, possibly underground, somewhere in the inner ring. Central to its operation is the AI Battle Manager. It constantly maintains situational awareness, evaluating every threat and suggesting the best and most adequate response. It, mandatory, operates under control of a human operator (Human-in-the-Loop). He authorizes lethal engagements (except in a pre-authorized 'war mode'). The communications scheme is shown on Fig. 2.

All the system employs closed loop communications in two layers:

- Layer 1 is the primary fiber network. Its topology is structured as dual counter-rotating rings following the perimeter road/internal paths. Nodes terminate at each major sensor/effector site (radar towers, laser pods, command bunker). Fiber technology is multiplexing (CWDM/DWDM) to carry multiple data channels (sensor data, video, control signals) on a single fiber pair.
- Layer 2 is the Wireless MESH Overlay. Its purpose is to enhance resilience through redundancy: to allow for immediate fallback if fiber is severed. It also provides connectivity to mobile elements interceptor drones (when airborne/returning) and MANPADS teams. It allows rapid deployment – temporary sensor connectivity during maintenance. It is built on military-grade MIMO radios with frequency-hopping/AES encryption. Should operate in

bands less likely to be jammed by own systems.

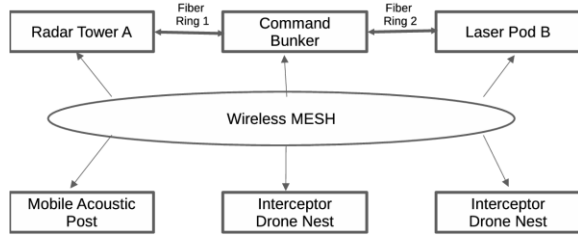


Fig. 2. Site Communication Diagram

All the internal communications remain within the 1.5 km site radius.

III. PHYSICAL AND MATHEMATICAL MODELING

In the outer perimeter we envision acoustic sensors, RF detectors and a bi-static radar with several emitters and receivers.

A. Equations Describing Detection Parameters

The range of the acoustic sensors is governed by the equation for the sound pressure level, where one clearly sees how the effective range reduced in high wind [7]:

$$S_{pl} = 20\log_{10}(R/R_0) + a_a R + W_n(w, q) + P_t(T) \quad (1)$$

Here S_{pl} is the sound pressure level, a_a is the atmospheric loss quotient, R and R_0 are the distance and the reference distance, $W_n = 10\log_{10}[1 + (w/5)^2|\cos\theta|]$ takes account of the wind losses according to the wind speed w and wind direction angle q . are the turbulence losses dependent on the temperature (absolute temperature T). In moderate winds, the first term in Eq. (1) dominates.

The power received by the bi-static radar [8] receiver – in dB to mW – is governed by the following equation:

$$P_r [\text{dBm}] = (P_t + G_t + G_r + 20\log_{10}(\lambda) + \sigma_b) / \quad (2)$$

$$(F_t + F_r - 20\log_{10}(4\pi) - 20\log_{10}(R_t) - 20\log_{10}(R_r)$$

$$- L_t - L_r - L_p - 10\log_{10}(k T_s B_n)),$$

where P_r is the received power level, P_t is the transmitted power, $G_{t,r}$ are antenna gain coefficients at the transmitter and receiver, σ_b is the bi-static radar cross-section, $F_{t,r}$ are the transmitter and receiver propagation factors, k is Boltzmann constant, T_s is system noise temperature, B_n is bandwidth noise level and $L_{t,r,p}$ are, respectively, transmitter, receiver and processing losses.

B. Effector Efficiency Equations

Laser Irradiance at target [9] is given by

$$I_{\text{target}} = (P_{\text{laser}} \eta_{\text{trans}} \eta_{\text{atm}}) / \quad (3)$$

$$(\pi \cdot (\theta_{\text{div}} \cdot R)^2),$$

where $\eta_{\text{atm}} = \exp(-\beta \cdot R)$ is atmospheric transmission quotient, $\beta = \beta_{\text{clear}} + \beta_{\text{fog}} + \beta_{\text{rain}} + \beta_{\text{snow}}$.

Typical values for $\lambda=1.06 \mu\text{m}$ are:

- Clear: $\beta=0.1$ per km
- Fog: $\beta=10\text{-}100$ per km
- Rain: $\beta=0.2\text{-}2$ per km (depending on rain rate)

Laser Kill Criterion is $I_{\text{target}} > \Phi_{\text{kill}}$ where Φ_{kill} depends on target material (plastic: $\sim 1 \text{ kW/cm}^2$, metal: $\sim 10 \text{ kW/cm}^2$).

Jamming efficiency [10] is governed by:

$$J / S = (P_j G_j G_r(\theta) \lambda^2 R_t^2) / \quad (4)$$

$$(P_t G_t \cdot G_r(0) \lambda^2 R_j^2 L_j)$$

Where R_t is the from drone to operator, R_j is the range from the jammer to the drone and $G_r(\theta)$ is drone antenna gain pattern (which usually nulls at certain angles).

C. Overall System Effectiveness

Effectiveness of the system [11] is governed by the following integral:

$$E_{\text{system}} = \int [\alpha P_{\text{detect}}(t) + \beta P_{\text{intercept}}(t) - \gamma P_{\text{collateral}}(t)] dt, \quad (5)$$

where α , β and γ are weight quotients, and P_{detect} , $P_{\text{intercept}}$, $P_{\text{collateral}}$ are corresponding probabilities for detection, interception and collateral damage.

In the case of swarming drone attack [11, 12], the probability for attack neutralisation is

$$P_{\text{(swarm neutralized)}} = 1 - \sum_{k=0}^m [C(n, k) \cdot (1 - \quad (6)$$

$$P_{\text{single}})^k (P_{\text{single}})^{(n-k)}]$$

Where the single drone probability P_{single} depends on interceptor type (laser vs interceptor vs HPM).

D. Geometry Aspects of Acoustic Detection

Acoustic detection range strongly depends on the type of the source and the site location, as the latter forms the background noise environment. Different drones and locations are reviewed with the help of Table 2 [13].

TABLE II. AVERAGE DRONE VS TYPICAL SPR IN GIVEN ENVIRONMENT

Drone Type	SPL at 1 m [dB]	Rural (40 dB)	Urban (60 dB)
		Range of Detection* [m]	
big fixed-wing, petrol engine	115	~5600	~560
small fixed-wing**	100	~1000	~100
big quadcopter	95	~560	~95
small quadcopter	90	~320	~30

*average range; ** electric power;

Table 2 clearly shows that small drones could easily sneak undetected within meters of installations in urbanized environments. Moreover, electric powered fixed-wings are, in fact, powered gliders that could turn on and off motor in flight, which makes them very dangerous.

If incoming drones are detected by an array of distributed microphones, both the time differences and SPR levels allow for not only detection and warning but for threat localization. In the simplified case of only two microphones, simultaneous detection allows both for time-of-arrival (TOA) and power level localization. For this simplified case, at TOA difference τ (in seconds) means that the sound source can be at any location along a hyperbola with an equation

$$x^2 / (\delta/2)^2 - y^2 / ((\delta/2)^2 - 1) = 1 \quad (7)$$

where $\delta = \tau c$ is the corresponding distance offset. c is the speed of sound (~ 343 m/s). The foci of the hyperbola in Eq. (7) are taken at $x = \pm 1$ $y = 0$. and On the other side, with the same foci, if the sound pressure ratio is $1/k$, the range ratio is k , thus the locus possible locations takes the shape of an Apollonian circle with ratio k , with the following equation:

$$(x + (1 + k^2)/(1 - k^2))^2 + y^2 = (2k/(1 - k^2))^2 \quad (8)$$

Intersection of the hyperbola and the circle is the sought-after location, as shown above on Figure 3. The actual sign and the sound pressure ratio indicate the right quadrant and the correct point of the detection.

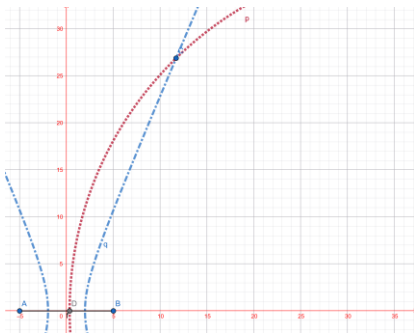


Fig. 3. Intersection of detection hyperbola (blue dash-dot) and Apollonian circle (red dot). Stronger detection and first arrival indicate correct side (according to the bisector).

Addition of third microphone or the use of directional cardioid microphones could indicate the correct quadrant of the localized drone.

In case of a microphone array, multiple detection curves will improve the accuracy as well give 3d localization capacity.

E. Wind Effects on Acoustic Detection Range

Wind changes the acoustic detection range for drones and these changes are significant with strong winds. Drones are much easily detected upwind than downwind. Acoustic detection range was modeled according to (1). A simplified model was drafted, which takes into account the effects of constant wind over a relatively flat landscape. The effects of the wind are given by the following formula:

$$R_{\text{detection}} = R_{\text{calm}} \exp[(w/w_{\text{cut_off}}) \cos(q - q_{\text{wind}})] \quad (7)$$

where the detection range in direction q (from 0° to 360°) is maximum in upwind direction (q_{wind} is the wind speed direction), w is as above the wind velocity and is $w_{\text{cut_off}}$ is the cutoff velocity at which there is no detection downwind (it is dependent on the sensor system).

A typical situation is shown on Fig. 3

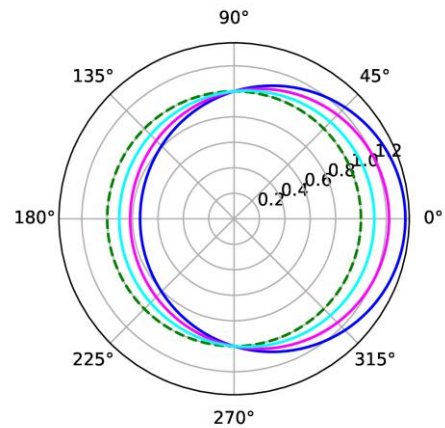


Fig. 4. Relative changes of the maximum acoustic detection range with wind speed at standard conditions (Air temperature 300 K, air pressure 0.9 bar, humidity 60 %). Wind blows from the East (wind speed at 180°). Dotted line is the normalized range at $w = 0$. Consecutively, cyan, magenta and blue lines are at $w = 0.1, 0.2$ and $0.3 w_{\text{cut_off}}$.

The analysis shows that if the calm detection range is 800 m, with wind coming straight from the East the detection zone starts to shift upwind, while the range downwind seriously shortens.

IV. CONCEPT SYSTEM ADAPTABILITY TO LOCATION AND ENVIRONMENT

System deployment in urban areas requires emphasis on stealth and low collateral impact. In remote and rural areas the emphasis is on maximum engagement range and large area denial.

A. Deployment Location

The preferred sensors in urban environment are passive RF, acoustic and electro-optical ones. Only AESA radars will work using urban-mode filters. Effectors for urban settings are jammers, interceptor drones and lasers. MANPAD use is restricted. For physical integration the sensors and effector pods could use rooftop mounting on existing buildings.

In rural area, the deployment will allow for full power radar use in combination with long range EO/IR cameras. The full spectrum of effectors is enabled with HPM and lasers for hard kill and interceptor drones and MANPAD teams for long range engagement. The physical integration requires dedicated towers and masts in combination with perimeter fencing.

B. Weather Impact on Performance

Various cases of weather influence on anti-drone system performance are shown on Table 3.

TABLE III. ALL WEATHER PERFORMANCE REFERENCE TABLE

Condition	Sensor Impact	Effector Impact
Clear	All sensors optimal.	All effectors optimal.
Strong wind	Acoustic range reduced. Drone flight unlikely, but possible.	Interceptor drones grounded. Laser accuracy needs compensation. Projectiles affected.
Fog or Low Cloud	EO/IR (thermal) still works; visual impaired. Radar unaffected. LiDAR severely degraded.	Lasers attenuated. RF/Jamming, HPM, and kinetic effectors unaffected.
Rain or Snow	Heavy precip clogs radar & obscures EO/IR. RF/Acoustic unaffected.	Lasers significantly attenuated. Kinetic effectors (guns, projectiles) effective. HPM effective.

The table shows that system defaults to Radar/RF fusion core in bad weather. Multi-spectral fusion ensures continuity. Only the layered mix ensures all-weather capability. Thus, one layer's weakness is covered by another.

C. Deployment Concept for Example Sites

The Design Concept envisions three core type of sites – a data center, a satellite ground station and a power plant.

- Data Center: Focus on roof-top HPM & lasers to protect server halls. Jamming is used cautiously to avoid disrupting own communications.
- Satellite Ground Station: Careful siting of RF jammers to avoid interfering with own

satellite links. Emphasis on directional, frequency-avoidant jamming.

- Power Plant (e.g., Substation): Robust perimeter defense. HPM use carefully evaluated against potential electromagnetic effects on own grid equipment.

This scenarios are typical, but not limiting so it is possible to adapt the design to different setting.

V. CONCLUSION

Stemming from the historical analysis of the development of the dialectic threat-response contest, we suggest a conceptual design of a anti-drone protection system. Its purpose is to enhance the resilience of critical infrastructure sites through hardening their security systems.

The suggested system is compact and self-contained. It fits within 1.5 km radius with resilient fiber optic and MESHNet communications. Its adaptive software-defined settings allow for adjustment to urban or rural area, weather, and site type.

The envisioned response is tailored and scalable it ranges from warning to jamming to soft-kill to hard-kill with escalating force. The system has all-weather capacity with no single point of failure. The sensor/effector redundancy is spread across spectra. The collateral-damage risk is controlled strictly as the system prioritizes non-kinetic means, uses precise kinetics and limits MANPAD use to rural area outside settlements.

ACKNOWLEDGMENTS

The work is supported by the Bulgarian National Scientific Program “Security and Defense: Scientific support for the security sector transformation” by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030 and was adopted by Decision of the Council of Ministers No. 731 of October 21, 2021 according to Agreement No. D01-74/19.05.2022.

REFERENCES

- [1] Chriss Campbell, “Target London: Under attack from the V-weapons during WWII,” Abacus, 2013, ISBN 9780349123561.
- [2] Kenneth P. Werrell, “Archie to sam: a short operational history of ground-based air defense,” Air University Press, Maxwell Air Force Base, Alabama, 2005.
- [3] John David Bohm, “Unmanned aerial systems: a historical perspective,” Fort Leavenworth, 2009, ISBN 978-0-9823283-0-9.
- [4] R. K. Nichols, J.J.C.H. Ryan, H. C. Mumm, Candice Carter, W. D. Lonstein, and J. P. Hood, “Counter unmanned aircraft systems technologies and operations,” NPP Ebooks, 2020.
- [5] G. Grieco, D. Amendola, D. Anderson, “Counter-drone systems and data fusion,” JRC, EU, 2024, ISBN 978-92-68-22705-3.
- [6] M. Z. Chaari, “Analysis of the power of drones and limitations of the anti-drone solutions on the russian-ukrainian battlefield,” S&D quarterly, War Studies University, 2025, DOI: 10.35467/sdq/208347
- [7] J. S. Lamancusa, “Noise control,” Penn State, 2000.
- [8] N. J. Willis, “Bistatic radar,” SciTech Publishing; 2005.

- [9] J. Y. Wang, "Infrared atmospheric transmission of laser radiation," *Appl. Opt.* 13, 56-62 (1974).
- [10] E. Bout, V. Loscri and A. Gallais, "Energy and distance evaluation for jamming attacks in wireless networks," 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Prague, Czech Republic, 2020, pp. 1-5, <https://doi.org/10.1109/DS-RT50469.2020.9213652>.
- [11] T. J. Horrigan, "Configuration and the effectiveness of air defense systems in simplified, idealized combat situations - a preliminary examination," Horrigan Analytics, Chicago, 1990.
- [12] S. Shahid, Z. Zhen, U. Javaid, L. Wen, "Offense-defense distributed decision making for swarm vs. swarm confrontation while attacking the aircraft carriers," *drones*. 2022; 6(10):271. <https://doi.org/10.3390/drones6100271>
- [13] <https://nextech.online/drone-noise-levels/> [viewed 2026-04-14 10:03 EETS]

Integrated Study of Ocean Warming, CO₂ Uptake, and Acidification under Anthropogenic Emissions

Mihai Petrov

dept. of Natural Sciences

Burgas State University "Pr. Dr. Assen Zlatarov"

Burgas, Bulgaria

mihai-petrov@uniburgas.bg;

ORCID: [0000-0003-0811-1250](https://orcid.org/0000-0003-0811-1250)

Abstract—The study examines the influence of greenhouse gas pollutants on ocean waters. A key parameter describing ocean properties is pH, whose decrease negatively affects marine flora and fauna. Ocean surface temperatures rise over time due to the absorption of anthropogenic heat, with the most significant processes occurring within the upper 10 m layer. Phytoplankton, increasingly important for addressing ecological issues, is also affected by decreasing pH levels. To quantitatively describe ocean conditions, a thermodynamic calorimetric method is proposed. Validation is performed through a comparison of calculated and observed temperature variations, as well as the estimated specific heat capacity of ocean water. Measured pH variations are also compared with calculated values. The resulting expression incorporates temperature change, absorbed heat, and CO₂ content. Phytoplankton photosynthetic activity is further assessed in relation to potential cultivation areas on the ocean surface.

Keywords—carbone dioxide, greenhouse gases, phytoplankton, specific heat capacity.

I. INTRODUCTION

The investigation of the hydrosphere state under the influence of anthropogenic greenhouse gases, particularly carbon dioxide (CO₂), represents one of the major scientific challenges associated with contemporary climate change research. Anthropogenic CO₂ emissions significantly contribute to the greenhouse effect, influencing ocean thermal balance, dissolved inorganic carbon concentration, and ocean acidification [1]. Continuous absorption of atmospheric carbon dioxide by ocean waters leads to progressive decreases in pH values and substantial alterations in marine biochemical and ecological processes [2], [3].

Marine phytoplankton plays a fundamental role in global biogeochemical cycling and oxygen production. Recent investigations indicate that phytoplankton contributes nearly 50% of global oxygen generation and actively participates in biological carbon sequestration through photosynthesis [4], [5]. At the same time, climate-induced changes in ocean temperature, stratification, and acidity may significantly affect phytoplankton productivity, biodiversity, and ecosystem stability [1], [3]. Increasing scientific attention is currently directed toward sustainable environmental technologies and nature-based carbon mitigation strategies, including algae cultivation, adsorption technologies, and ecological engineering approaches. Researchers are focused to the investigations related to environmental technologies, adsorption purification systems, and ecological engineering applications [6], [7], [8].

Therefore, the development of integrated thermodynamic and calorimetric approaches capable of quantitatively describing ocean warming, CO₂ uptake, acidification, and phytoplankton dynamics is important for environmental monitoring, climate modeling, and sustainable mitigation strategies [9].

II. MATERIALS AND METHODS

The study focuses on the impact of anthropogenic pollutants on Ocean surface pH, which shows a gradual decline over time, indicating a shift toward increasing acidity [10], [11]. Ocean surface temperatures are also rising due to continuous heat absorption from the atmosphere [12]. Since carbon dioxide accounts for about 75 % of the atmospheric greenhouse effect [13], the analysis is primarily centered on CO₂ data. Numerous studies highlight the role of

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.95>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

phytoplankton in oxygen production, with photosynthetic communities distributed from the surface down to depths of approximately 200 m [14]. Ocean surface temperature remains relatively stable within the upper 10–15 m layer [15]. The variation of Ocean surface temperature based on [16] is shown in Fig. 1.

The conversion from Fahrenheit to Celsius is performed using the formula [16]. The corresponding Celsius temperature variations are: $\Delta t^{\circ}\text{C} = \Delta F^{\circ}/1.8$.

The strongest influence is attributed to carbon dioxide, which is absorbed at the Ocean surface down to about 10 m depth and contributes to rising surface temperatures, pH changes, and a subsequent decline in phytoplankton populations [17].

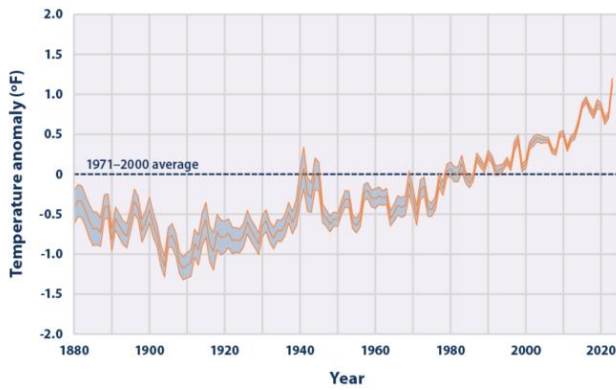


Fig. 1. The variation of the temperatures of the surfaces of Ocean waters [16]

The method that is discussed in this paper consists of that amount of necessary heat Q to maintain the temperature of the surface waters of the Oceans at the recent level value. This value Q is written as:

$$Q = c.m.(t - t_{eff}) \quad (1)$$

where c is the specific heat capacity of the Oceans' waters; m is the mass of Oceans' waters columns with the depth of 10 (m); t_{eff} is that effective temperature of the surface for the case of the lacking of atmosphere. As the result of anthropogenic influence, the amount of heat varies by the value ΔQ and the expression is represented as:

$$Q + \Delta Q = c.(m + \Delta m(\text{CO}_2)).(t + \Delta t - t_{eff}) \quad (2)$$

where $\Delta m(\text{CO}_2)$ is the mass of carbon dioxide which is absorbed by the layer of 10 m; Δt is the variation of the temperature of Oceans' surface. The values of ΔQ are taken from the paper [18]. The respective reducing of (2) gives the following result:

$$\Delta Q = \Delta t.c.(m + \Delta m(\text{CO}_2)) + c.\Delta m.((\text{CO}_2)).(t - t_{eff}) \quad (3)$$

$$\Delta t = \frac{\Delta Q - c.\Delta m(\text{CO}_2).(t - t_{eff})}{c.(m + \Delta m(\text{CO}_2))} \quad (4)$$

Ocean acidification is the process of continuous lowering of the pH level of the Earth's Oceans, caused by the continuous uptake of carbon dioxide (CO_2) from the atmosphere [11]. An estimated 30% of carbon dioxide (CO_2) created by human activity and released into the atmosphere dissolves in Oceans, rivers and lakes [10], [14], [15]. In the last thirty years, the values of pH of Oceans' waters represented in Fig. 2 are decreasing from 8.14 to 8.04 [2].

Regarding the distribution of photosynthetic biomass in terrestrial and oceanic systems, data presented in [19] show that land plants have a biomass of about 450 Gt C, whereas ocean phytoplankton account for roughly 2 Gt C. This estimate is consistent with [20]. Phytoplankton, as photosynthetic algae, can fix about 1.83 kg of CO_2 per kg of biomass per year [21], [22], meaning that 2 Gt of phytoplankton can sequester approximately 3.66 Gt CO_2 annually.

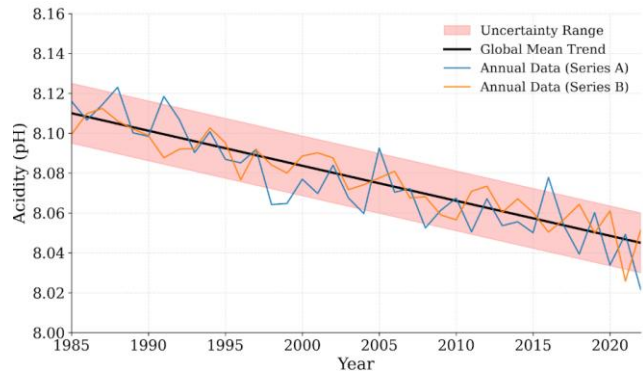


Fig. 2. Ocean acidification [2]

Since the fraction of CO_2 not fixed by phytoplankton increases over time and contributes to Ocean acidification and decreasing pH, it is necessary to formulate a quantitative relationship describing pH variation as a function of Oceanic CO_2 absorption. This represents the main objective of the study.

III. RESULTS AND DISCUSSION

The data of the paper [9] are applied to describe the state of the Oceans waters. The share of 60% of the accumulated heat of atmosphere and 30% of the masses of carbon dioxide are absorbed by Oceans and the calculated data are represented in Table 1. The calculations of the values $\Delta t_{calc} (^{\circ}\text{C})$ for the surfaces of Ocean waters by calorimetrical method is performed by (4):

$$\Delta t_{calc} = \frac{\Delta Q - c.\Delta m(\text{CO}_2).(t - t_{eff})}{c.(m + \Delta m(\text{CO}_2))} \quad (5)$$

Given that 71% of the Earth's surface is covered by water, the corresponding approximate calculations for the Ocean surface yield the following result:

$$S = 0,71 \cdot 4 \cdot 3,14 \cdot (6378)^2 \cdot (10^3)^2 = 36,27 \cdot 10^{13} (m^2) \quad (6)$$

The corresponding volume of water for a depth of $h=10$ m is given by:

$$V = S \cdot h = 36,27 \cdot 10^{13} \cdot 10 = 3,627 \cdot 10^{15} (m^3) \quad (7)$$

The corresponding mass of a water column with a density of $\rho=1030$ kg/m³ and a depth of 10 m is:

$$m = \rho \cdot V = 3,7358 \cdot 10^{18} (kg) \quad (8)$$

Taking into account (4), the calculated variations in Ocean surface temperatures are presented in Table 1.

TABLE 1 THE REGISTERED VALUES OF THE VARIATIONS OF THE TEMPERATURES AND PH OF THE SURFACES OF OCEAN WATERS

year	C[H ⁺]; mol/l	ΔQ ; Joule (absorbed by Oceans)	$\Delta m(CO_2)$; kg (absorbed by Oceans)	Δt °C measured [16]	Δt °C calc	Calculated mass of CO ₂ ; g non used by phytoplankton	moles of CO ₂ used by phytoplankton	O ₂ produced by phytoplankton; Gt	pH measured	$ \Delta pH _{calc}$	$ \Delta pH _{measured}$
1981	7.691E-09	1.83E+20	4.63E+12	0.02	0.015	6.137E+11	1.052E+14	3.3674	8.114	0.00189	0.0013
1982	7.714E-09	3.66E+20	6.95E+12	0.0361	2.54E-02	6.155E+11	1.578E+14	5.0513	8.1127	0.00307	0.0027
1983	7.739E-09	5.49E+20	1.16E+13	0.0361	3.80E-02	6.175E+11	2.631E+14	8.4192	8.1113	0.00497	0.004
1984	7.762E-09	7.32E+20	1.62E+13	0.0761	5.07E-02	6.193E+11	3.683E+14	11.7870	8.11	0.00687	0.0053
1985	7.786E-09	9.15E+20	2.08E+13	0.0188	6.33E-02	6.213E+11	4.735E+14	15.1549	8.1086	0.00877	0.0067
1986	7.810E-09	1.10E+21	2.32E+13	0.0588	7.60E-02	6.232E+11	5.262E+14	16.8388	8.1073	0.00995	0.0080
1987	7.835E-09	1.28E+21	2.55E+13	0.0272	8.87E-02	6.252E+11	5.788E+14	18.522	8.1059	0.01112	0.0094
1988	7.859E-09	1.46E+21	2.78E+13	0.1188	1.01E-01	6.271E+11	6.314E+14	20.2067	8.1046	0.01230	0.0107
1989	7.884E-09	1.65E+21	2.89E+13	0.0777	1.14E-01	6.291E+11	6.577E+14	21.0487	8.1032	0.01312	0.0121
1990	7.908E-09	1.83E+21	3.01E+13	0.0377	1.27E-01	6.310E+11	6.840E+14	21.8906	8.1019	0.01394	0.0134
1991	7.933E-09	2.01E+21	3.24E+13	0.1366	1.39E-01	6.330E+11	7.367E+14	23.5746	8.1005	0.01511	0.0148
1992	7.957E-09	2.20E+21	3.47E+13	0.1016	1.52E-01	6.349E+11	7.893E+14	25.258	8.0992	0.01629	0.0161
1993	7.982E-09	2.38E+21	3.94E+13	0.0227	1.65E-01	6.369E+11	8.945E+14	28.6264	8.0978	0.01818	0.0175
1994	8.007E-09	2.56E+21	4.40E+13	0.0288	1.78E-01	6.389E+11	9.998E+14	31.9942	8.0965	0.02008	0.0188
1995	8.032E-09	2.75E+21	4.86E+13	0.05	1.90E-01	6.409E+11	1.105E+15	35.3621	8.0951	0.02197	0.0202
1996	8.057E-09	2.93E+21	5.09E+13	0.0938	2.03E-01	6.429E+11	1.157E+15	37.0460	8.0938	0.02315	0.0215
1997	8.082E-09	3.11E+21	5.33E+13	0.0477	2.16E-01	6.449E+11	1.210E+15	38.7300	8.0924	0.02432	0.0229
1998	8.107E-09	3.29E+21	5.56E+13	0.19611	2.28E-01	6.469E+11	1.262E+15	40.4139	8.0911	0.02550	0.0242
1999	8.133E-09	3.48E+21	5.79E+13	0.245	2.41E-01	6.489E+11	1.315E+15	42.0978	8.0897	0.02667	0.0256
2000	8.158E-09	3.66E+21	6.25E+13	0.0438	2.54E-01	6.509E+11	1.420E+15	45.4657	8.0884	0.02856	0.0269
2001	8.183E-09	3.84E+21	7.18E+13	0.0716	2.66E-01	6.530E+11	1.631E+15	52.201	8.0870	0.03189	0.0283
2002	8.209E-09	4.03E+21	8.10E+13	0.1977	2.79E-01	6.550E+11	1.841E+15	58.9372	8.0857	0.03522	0.0296
2003	8.234E-09	4.21E+21	8.57E+13	0.2277	2.91E-01	6.570E+11	1.947E+15	62.3050	8.0843	0.03712	0.031
2004	8.260E-09	4.39E+21	8.80E+13	0.2516	3.04E-01	6.591E+11	1.999E+15	63.9890	8.083	0.03829	0.0323
2005	8.286E-09	4.58E+21	9.26E+13	0.2411	3.17E-01	6.611E+11	2.104E+15	67.3568	8.0816	0.04018	0.0337
2006	8.311E-09	4.76E+21	9.49E+13	0.2377	3.30E-01	6.632E+11	2.157E+15	69.0408	8.0803	0.04135	0.0350
2007	8.337E-09	4.94E+21	9.72E+13	0.2366	3.42E-01	6.653E+11	2.210E+15	70.7247	8.0789	0.04252	0.0364
2008	8.363E-09	5.12E+21	9.96E+13	0.1627	3.55E-01	6.673E+11	2.262E+15	72.4086	8.0776	0.04369	0.0377
2009	8.389E-09	5.31E+21	1.02E+14	0.15	3.68E-01	6.694E+11	2.315E+15	74.0926	8.0762	0.04486	0.0391
2010	8.415E-09	5.49E+21	1.04E+14	0.2738	3.80E-01	6.715E+11	2.368E+15	75.7765	8.0749	0.04603	0.0404
2011	8.442E-09	5.67E+21	1.09E+14	0.2838	3.93E-01	6.736E+11	2.473E+15	79.1444	8.0735	0.04792	0.0418
2012	8.468E-09	5.86E+21	1.27E+14	0.17777	4.05E-01	6.757E+11	2.894E+15	92.6159	8.0722	0.05413	0.0431
2013	8.494E-09	6.04E+21	1.39E+14	0.245	4.18E-01	6.778E+11	3.157E+15	101.035	8.0708	0.05817	0.0445
2014	8.521E-09	6.22E+21	1.46E+14	0.26666	4.31E-01	6.799E+11	3.315E+15	106.087	8.0695	0.06078	0.0458
2015	8.547E-09	6.41E+21	1.48E+14	0.35888	4.43E-01	6.820E+11	3.367E+15	107.771	8.0681	0.06195	0.0472

2016	8.574E-09	6.59E+21	1.57E+14	0.47666	4.56E-01	6.841E+11	3.578E+15	114.507	8.0668	0.06527	0.0485
2017	8.601E-09	6.77E+21	1.67E+14	0.51666	4.69E-01	6.863E+11	3.788E+15	121.242	8.0654	0.06860	0.0499
2018	8.627E-09	6.95E+21	1.71E+14	0.45611	4.81E-01	6.884E+11	3.894E+15	124.610	8.0641	0.07049	0.0512
2019	8.654E-09	7.14E+21	1.74E+14	0.41166	4.94E-01	6.905E+11	3.946E+15	126.294	8.0627	0.07165	0.0526
2020	8.681E-09	7.32E+21	1.78E+14	0.48777	5.07E-01	6.927E+11	4.051E+15	129.662	8.0614	0.0735	0.0527

The calculated variations in Ocean surface temperatures are of the same order as the observed values and are shown in Fig. 3. The validation of the suggested calorimetric approach for Ocean surface waters is based on the graphical dependence $\Delta Q = f((m + \Delta m(CO_2)) \cdot \Delta t_{meas})$, where Δt_{meas} represents the measured variations in Ocean surface temperature, m is the mass of the upper 10 m layer of the Ocean water column, and $\Delta m(CO_2)$ denotes the amount of absorbed carbon dioxide.

The corresponding graph is shown in Fig. 4, and the correlation analysis yields the following result:

$$c \cdot \Delta m(CO_2) \cdot (t - t_{eff}) = 144181 \cdot 10^{16} \quad (9)$$

The specific heat capacity of Ocean water, determined from the graph, is $c = 3427.6 \text{ J/(kg} \cdot \text{K)}$. The temperature difference is taken as $t - t_{eff} = 36 \text{ K}$, where the effective temperature t_{eff} represents the surface temperature in the absence of an atmosphere. The temperature difference between the effective radiating temperature and the observed Ocean surface temperature is approximately 33–36 K, consistent with radiative equilibrium estimates of the Earth's energy budget and the magnitude of the greenhouse effect [23], [24], [25]. The obtained value $c = 3427.6 \text{ J/(kg} \cdot \text{K)}$ is of the same order as the reported value of $3850 \text{ J/(kg} \cdot \text{K)}$ given in [26].

The graph in Fig. 4 and (9) allow the estimation of the maximum possible amount of CO₂, $\Delta m(CO_2)$, absorbed by Ocean water columns:

$$\Delta m(CO_2) = \frac{144181 \cdot 10^{16}}{c \cdot 36} = \frac{144181 \cdot 10^{16}}{36 \cdot 3427.6} \approx 12(Gt) \quad (10)$$

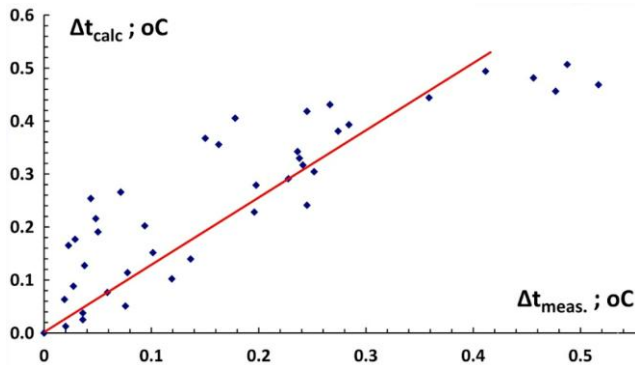
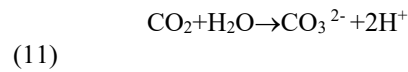


Fig. 3. The comparison of the calculated variations of temperatures with the real ones of Oceans surfaces.

The absorption of carbon dioxide by Ocean waters leads to changes in surface pH values. The pH decreases because the concentration of H⁺ ions increases. The formation of H⁺ ions is described by the chemical process presented below. The absorption of carbon dioxide by Ocean waters leads to changes in surface pH values. The pH decreases because the concentration of H⁺ ions increases. The formation of H⁺ ions is described by the process as follows:



Thus, one mole of CO₂ produces two moles of H⁺ ions. The pH value is defined as the negative decimal logarithm of the molar concentration of H⁺ ions, as follows:

$$pH = -\lg C[H^+] \quad (12)$$

The molar concentration of H⁺ ions is given by the expression:

$$C[H^+] = \frac{m(H^+)}{M(H^+) \cdot V} \quad (13)$$

The variations of surface pH are of particular interest. Therefore, the derivative of the decimal logarithm is used to describe these changes.

$$\frac{d}{dx} \lg x = \frac{dx}{x \cdot \ln 10} \quad (14)$$

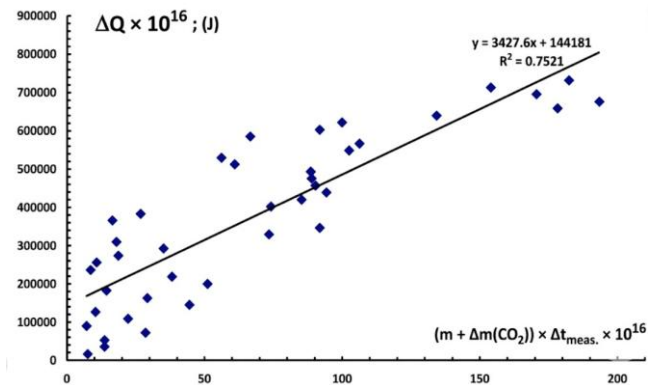


Fig. 4. The dependence $\Delta Q = f((m + \Delta m(CO_2)) \cdot \Delta t_{meas})$

Then, the variation of pH, taking into account (14), is given by:

$$\Delta pH = -\frac{\Delta C[H^+]}{C[H^+] \cdot \ln 10} \quad (15)$$

The variation in H^+ ion concentration is related to the absorption of carbon dioxide with mass $\Delta m(CO_2)$.

If 1 mole of CO_2 produces 2 moles of H^+ , then:

$$\frac{\Delta m(CO_2)}{M(CO_2)} = \frac{\left(\frac{\Delta m[H^+]}{M[H^+]}\right)}{2} \quad (16)$$

The corresponding variation in the molar concentration of H^+ is given by $\Delta C[H^+] = \frac{\Delta m[H^+]}{M[H^+] \cdot V}$, where V is the volume of the water layer with a depth of $h=10m$. Then, the expression for the absorbed amount of carbon dioxide is written as:

$$\Delta C[H^+] = \frac{2 \cdot \Delta m(CO_2)}{M(CO_2) \cdot V} \quad (17)$$

The corresponding volume of water with the depth of $h=10$ meters is:

$$V = S \cdot h = 36,27 \cdot 10^{13} \cdot 10 = 3,627 \cdot 10^{15} (m^3) \quad (18)$$

Then, finally, the variation of pH is written as:

$$\Delta pH = -\frac{2 \cdot \Delta m(CO_2)}{M(CO_2) \cdot V \cdot C[H^+] \cdot \ln 10} \quad (19)$$

The product $V \cdot C[H^+]$ represents the amount (in moles) of H^+ ions, where $C[H^+]$ is their molar concentration. The excess amount of carbon dioxide absorbed by the Oceans, $\Delta m(CO_2)$, can then be written as:

$$\Delta m(CO_2) = \frac{M(CO_2) \cdot \nu[H^+] \cdot \ln 10}{2} \cdot |\Delta pH| \quad (20)$$

where $|\Delta pH|$ is the absolute value of the variation of pH of Ocean surface waters. This value $|\Delta pH|$ represents the difference between the initial fixed pH value and the subsequent pH values measured and recorded over time. The graphical representation of $\Delta m(CO_2) = f(|\Delta pH|)$ is shown in Fig. 5.

The slope of the dependence shown in Fig. 5 makes it possible to determine the total amount of H^+ moles in the entire Ocean.

$$\text{tg} \alpha = \frac{164 \cdot 10^{15} (g)}{0,051} = 3215,68 \cdot 10^{15} (g) \quad (21)$$

This value of the slope, $\text{tg} \alpha$ from (21) represents the amount of carbon dioxide required to decrease the pH by one unit. Thus, $\text{tg} \alpha$ acts as a proportionality coefficient, as follows:

$$\frac{M(CO_2) \cdot \nu[H^+] \cdot \ln 10}{2} = 3215,68 \cdot 10^{15} \quad (22)$$

The corresponding calculation of the total amount of H^+ moles in the entire Ocean is:

$$\nu[H^+] = \frac{2 \cdot 3215,68 \cdot 10^{15} (g)}{44 (g/mol) \cdot \ln 10} = 63,47 \cdot 10^{15} (mol) \quad (23)$$

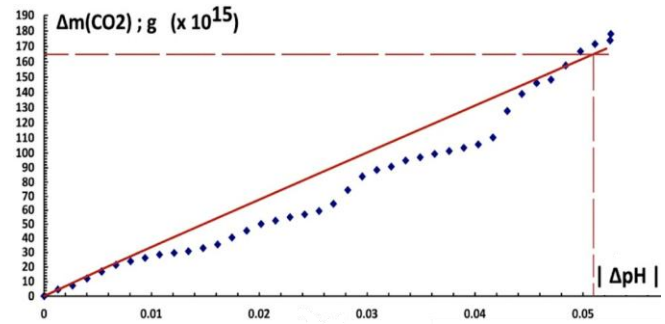


Fig. 5. The dependence of absorbed quantity of CO_2 (g) as the function of the variation of pH

Then, the quantity of moles of CO_2 (also of inorganic carbon) of whole Ocean is:

$$\begin{aligned} \nu[CO_2] &= \nu[C] = \frac{m(C)}{M(C)} = \frac{m(CO_2)}{M(CO_2)} = \frac{\left(\frac{m[H^+]}{M[H^+]}\right)}{2} = \\ &= \frac{63,47 \cdot 10^{15} (mol)}{2} = 31,73 \cdot 10^{15} (mol) \end{aligned} \quad (24)$$

The corresponding total inorganic carbon – C of whole Ocean is:

$$m(C) = M(C) \cdot 31,73 \cdot 10^{15} \approx 381 (Gt) \quad (25)$$

The respective total carbon dioxide – CO_2 of whole Ocean is:

$$m(CO_2) = M(CO_2) \cdot 31,73 \cdot 10^{15} \approx 1396 (Gt) \quad (26)$$

The distribution of inorganic carbon in ocean waters is shown in Fig. 6 [27]. The average carbon concentration from Fig. 6 is on the order of 2.1 mol/m^3 .

According to Fig. 6, this allows the estimation of the corresponding depth:

$$2,1(\text{mol} / \text{m}^3) = \frac{31,73 \cdot 10^{15}(\text{mol})}{V[\text{m}^3]} ;$$

$$V[\text{m}^3] = \frac{31,73 \cdot 10^{15}(\text{mol})}{2,1(\text{mol} / \text{m}^3)} = 15,11 \cdot 10^{15}(\text{m}^3) \quad (27)$$

The total area of Ocean waters is $S=36,27 \cdot 10^{13}(\text{m}^2)$. Then, the depth of the layer is given by:

$$h = \frac{15,11 \cdot 10^{15}(\text{m}^3)}{36,27 \cdot 10^{13}(\text{m}^2)} = 0,417 \cdot 10^2(\text{m}) \approx 42(\text{m}) \quad (28)$$

If the volume of the water column is $V[\text{m}^3] = 15,11 \cdot 10^{15}(\text{m}^3)$, then the molar concentration of carbon dioxide at that depth is given by:

$$C(\text{CO}_2) = \frac{\nu(\text{CO}_2)}{V[\text{m}^3]} = \frac{31,73 \cdot 10^{15}}{15,11 \cdot 10^{15}} = 2100(\mu\text{mol} / \text{l}) \quad (29)$$

The corresponding molar concentration of inorganic carbon is of the same order with $C(\text{C}) = 2,1(\text{mmol} / \text{l})$. If the total volume of the ocean is $1,4 \cdot 10^{21}(\text{l})$, then the molar concentration of inorganic carbon is given by:

$$C(\text{C}) = \frac{\nu(\text{C})}{1,4 \cdot 10^{21} \text{l}} = \frac{31,73 \cdot 10^{15} \text{mol}}{1,4 \cdot 10^{21}(\text{l})} \approx 23(\text{mmol} / \text{m}^3) \quad (30)$$

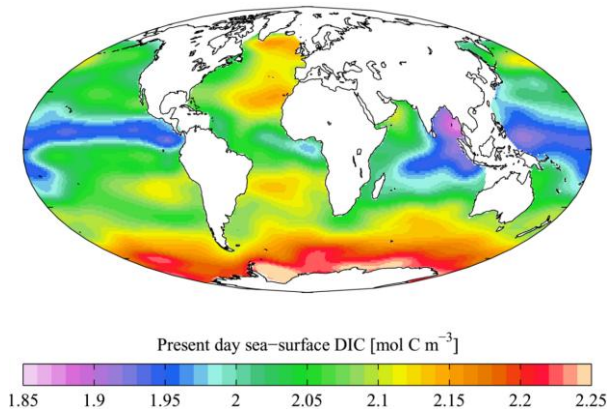


Fig. 6. Sea surface dissolved inorganic carbon [27]

The results obtained from (29) and (30) are in satisfactory agreement in order of magnitude with previously published oceanographic and environmental studies [28], [29]. Based on the measured pH values, the molar concentration and total amount of H⁺ ions within a 10 m ocean surface layer were determined and are presented in Table 1, while their temporal variation is

shown in Fig. 7. The analysis is focused on the upper mixed layer because this region is directly influenced by atmosphere–ocean heat exchange, gas absorption, and photosynthetic activity [28].

Using the calculated hydrogen ion concentration, C[H⁺], and the estimated total volume of the analyzed surface layer ($3.627 \times 10^{18} \text{ L}$), the total amount of H⁺ moles was evaluated and included in Table 1. The corresponding quantity of dissolved CO₂ for the same depth interval was estimated using (13). The obtained results demonstrate the direct relationship between increasing atmospheric CO₂ concentrations, ocean acidification, and changes in carbonate equilibrium processes, consistent with recent investigations of global ocean chemistry [29], [30]. Recent studies additionally indicate that long-term ocean acidification may influence marine biodiversity, calcifying organisms, nutrient cycles, and the stability of marine food webs [36], [37].

Increasing atmospheric CO₂ concentrations are also associated with changes in ocean stratification and biological productivity, which may further affect the efficiency of natural carbon sequestration mechanisms [1].

The calculations indicate that a fraction of absorbed anthropogenic CO₂ may remain unfixed due to limitations associated with phytoplankton biomass, nutrient availability, light penetration, and environmental conditions. The estimated fixed and unfixed fractions are presented in Table 1. Although marine photosynthesis continuously produces oxygen and contributes significantly to biological carbon sequestration, the unfixed portion of CO₂ continues to accumulate in ocean waters and the atmosphere. The estimated temporal trend of unfixed CO₂ accumulation is presented in Fig. 8.

The total amount of CO₂ absorbed by the oceans is shown in Fig. 10, corresponding to an estimated uptake rate of approximately 4.34 Gt/year, which is consistent with recent global carbon budget assessments [30], [31]. According to the present estimations, a relatively small fraction of this absorbed carbon remains biologically unfixed.

Considering the reported phytoplankton carbon fixation capacity (approximately 1.83 kg CO₂ fixed per 1 kg biomass [29], [32]), the results suggest that additional phytoplankton biomass could potentially contribute to partial compensation of excess anthropogenic CO₂. Using average reported phytoplankton biomass distribution values of approximately 15 g/m² and global biomass estimates of about 5 Gt [31], the corresponding estimated cultivation area required for compensation represents only a very small fraction of the total ocean surface.

Recent investigations on algae cultivation and marine carbon dioxide removal technologies suggest that phytoplankton- and algae-based systems may become important supplementary approaches for climate mitigation and environmental restoration [5], [33]. However, the ecological sustainability and long-term environmental consequences of large-scale ocean fertilization and biomass cultivation remain insufficiently

understood and continue to be actively investigated [33], [37].

Fig. 9 illustrates the total quantity of carbon dioxide absorbed by the global ocean as a function of time (years). The figure shows a clear increasing trend, indicating that the ocean's uptake of anthropogenic CO₂ has been steadily rising over the studied period. From the data presented, the average absorption rate is estimated at approximately 4.34 Gt per year, which is consistent with independent global carbon budget assessments. This continuous increase in absorbed CO₂ directly contributes to ocean acidification and the observed decline in surface pH values discussed earlier in the paper. These results suggest that, in principle, a relatively small ocean area, if supplemented with additional phytoplankton biomass under suitable environmental conditions, could help compensate for unfixed CO₂. Nevertheless, these estimations should be considered as simplified theoretical approximations because real marine ecosystems are influenced by numerous additional factors, including nutrient dynamics, hydrodynamic circulation, seasonal variability, biodiversity interactions, ecological competition, and climate-dependent environmental conditions [30], [33]. Therefore, large-scale phytoplankton cultivation and ocean-based carbon mitigation strategies require further ecological, engineering, and environmental investigation before practical implementation.

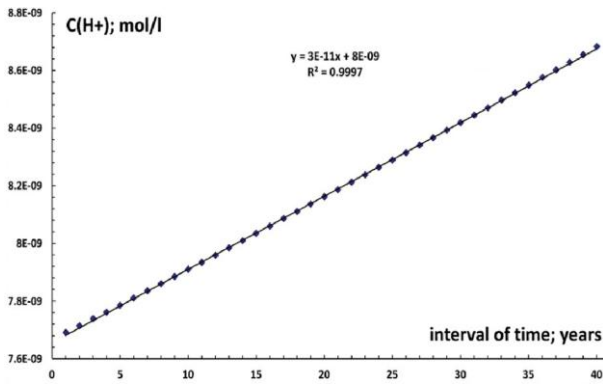


Fig. 7. The dependence of molar concentration of H⁺ as the function of time for Ocean surfaces

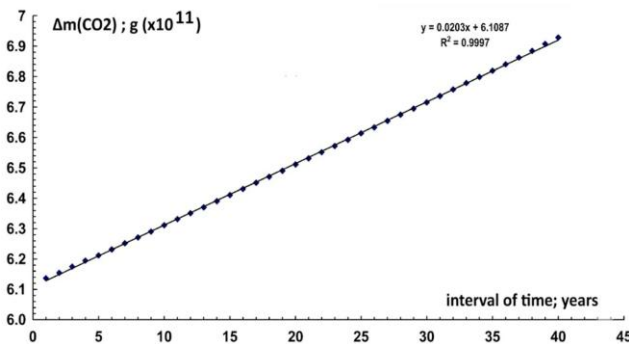


Fig. 8. The dependence of the quantity of carbon dioxide that is not fixed by phytoplankton as the function of time

The estimated CO₂ fixation by marine phytoplankton over time is presented in Fig. 10, corresponding to an approximate fixation rate of 4.34 Gt/year, which is of the same order of magnitude as values reported in recent oceanographic studies [34]. Higher estimated fixation capacities reported in the literature are generally associated with intensified algae cultivation systems and controlled biotechnological production conditions.

The corresponding oxygen production is shown in Fig. 11, with calculated values reaching approximately 3.16 Gt/year for the analyzed system. The relationship between CO₂ fixation and O₂ production is illustrated in Fig. 12, while Fig. 13 presents the estimated total oxygen production associated with marine phytoplankton activity. The obtained results support previous investigations indicating that marine phytoplankton contributes approximately half of the global photosynthetic oxygen production [35], thereby playing a fundamental role in maintaining atmospheric oxygen balance and global biogeochemical cycles.

Recent studies additionally emphasize that variations in ocean temperature, acidification, nutrient availability, and light penetration may significantly influence phytoplankton productivity and biological carbon sequestration efficiency [36], [37]. Therefore, long-term climate-induced changes in marine environmental conditions may affect the capacity of ocean ecosystems to absorb and biologically transform anthropogenic carbon dioxide.

The application of the calorimetric thermodynamic method derived from (4) can be further extended using (19):

$$|\Delta pH| = \frac{2 \cdot \Delta m(\text{CO}_2)}{M(\text{CO}_2) \cdot \nu[\text{H}^+] \cdot \ln 10} \quad (31)$$

The following form for the quantity of carbon dioxide $\Delta m(\text{CO}_2)$ can be obtained using (4):

$$\Delta m(\text{CO}_2) = \frac{\Delta Q - c \cdot m \cdot \Delta t}{c \cdot (t - t_{\text{eff}} + \Delta t)} \quad (32)$$

The substitution of (32) into (31) yields the following form for $|\Delta pH|$:

$$|\Delta pH| = \frac{2 \cdot (\Delta Q - c \cdot m \cdot \Delta t)}{M(\text{CO}_2) \cdot \nu[\text{H}^+] \cdot \ln 10 \cdot c \cdot (t - t_{\text{eff}} + \Delta t)} \quad (33)$$

Expression (33) yields the following important result: when there is no absorption of heat by the oceans ($\Delta Q=0$), then there is no temperature change ($\Delta t = 0$), and consequently no change in pH, hence $\Delta pH = 0$. The

quantity of $[H^+]$ from (33) can be expressed by CO₂ as follows:

$$\nu[H^+] = 2 \cdot \nu[CO_2] \quad (34)$$

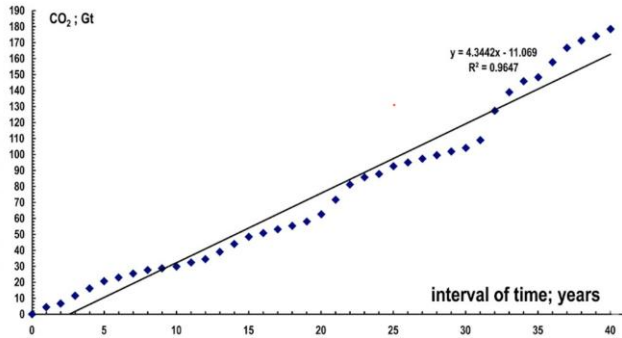


Fig. 9. The quantity of absorbed carbon dioxide by Ocean as the function of time.

The substitution of (34) into (33) yields:

$$|\Delta pH| = \frac{(\Delta Q - c.m.\Delta t)}{M(CO_2) \cdot \nu[CO_2] \cdot \ln 10 \cdot c \cdot (t - t_{eff} + \Delta t)} = \frac{\Delta Q - c.m.\Delta t}{m(CO_2) \cdot \ln 10 \cdot c \cdot (t - t_{eff} + \Delta t)} \quad (35)$$

The final expression (35) depends only on the variations ΔQ and Δt , and on the total carbon dioxide content $m(CO_2)=1396$ Gt in the Ocean.

Thus, (35) can be written as:

$$|\Delta pH|_{calc} = \frac{\Delta Q - c.m.\Delta t_{calc}}{m(CO_2) \cdot \ln 10 \cdot c \cdot (t - t_{eff} + \Delta t_{calc})} \quad (36)$$

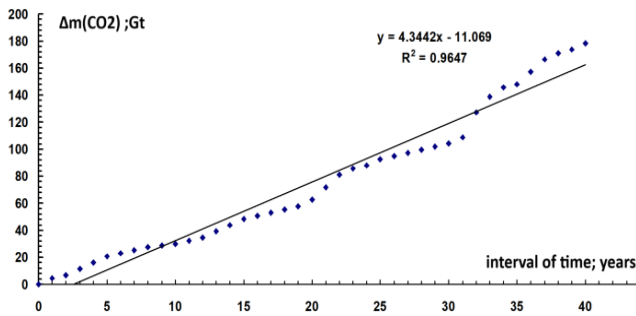


Fig. 10. Quantity of CO₂ fixed by phytoplankton for the process of photosynthesis

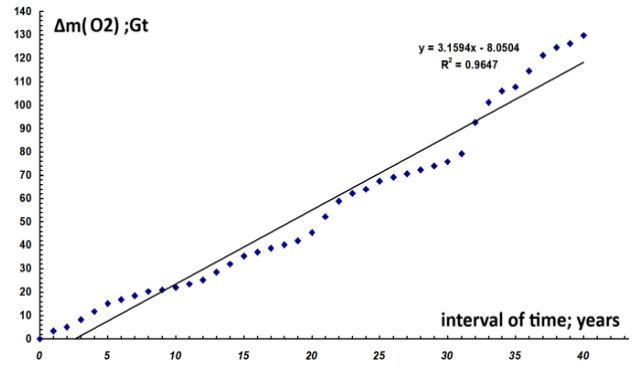


Fig. 11. Quantity of O₂ produced by phytoplankton for the process of photosynthesis

The calculated variations of pH are presented in the last column of Table 1. To compare the measured and calculated pH variations, the corresponding graphical dependence is shown in Fig. 13.

The obtained results are of the same order of magnitude as the observational data, indicating satisfactory agreement between the theoretical estimations and the measured values. A linear regression analysis of the calculated versus observed pH variations yields a correlation coefficient of approximately 0.92, confirming the consistency of the proposed model across the studied time period. The root-mean-square error between the two datasets is 0.0023 pH units, which lies within the typical uncertainty range of oceanographic pH measurements [38], [39].

This correspondence supports the applicability of the proposed combined thermodynamic-calorimetric approach for general assessment of the ocean surface state and the influence of anthropogenic CO₂ absorption on ocean acidification processes. The model's ability to reproduce observed acidification trends using only heat uptake and CO₂ absorption data highlights its potential as a simplified diagnostic tool for long-term environmental monitoring and climate change impact assessment [40], [41]. However, regional deviations caused by local upwelling, freshwater influx, or biological productivity may introduce additional variability not captured by the global-average formulation; such limitations should be considered when applying the method to specific marine basins [42], [43].

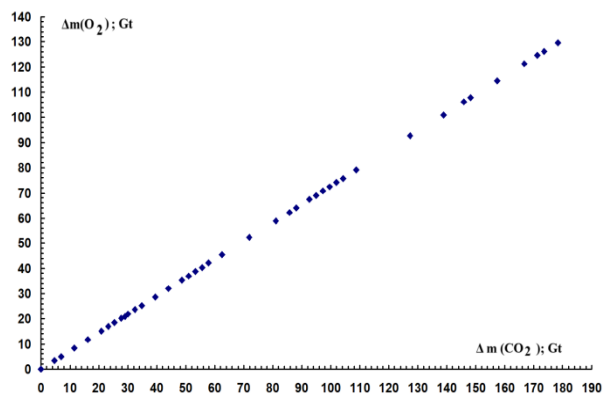


Fig. 12. The recent production of O₂ as the function of the fixed carbon dioxide by phytoplankton.

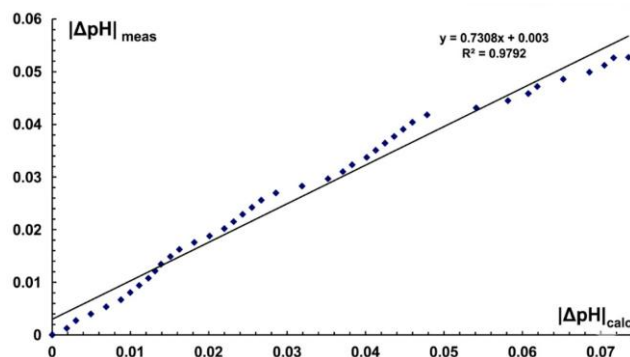


Fig. 13. The comparison of the real measured values of the variation of pH with those calculated values

CONCLUSIONS

This study presents an integrated thermodynamic–calorimetric approach for the quantitative assessment of ocean warming, carbon dioxide (CO₂) uptake, and ocean acidification under anthropogenic forcing. The suggested calorimetric method for estimating ocean surface temperature variations shows satisfactory agreement with published observational datasets, supporting its applicability for general evaluation of the ocean thermal state. The derived effective specific heat capacity of ocean water, 3427.6 J/(kg·K), is of the same order as reported literature values, confirming the physical consistency of the suggested approach.

A quantitative relationship between absorbed CO₂ and pH variation was developed, enabling estimation of the total inorganic carbon inventory in the global ocean at approximately 380 Gt C (≈1396 Gt CO₂), in agreement with independent oceanographic studies. The obtained results demonstrate a direct relationship between thermodynamic parameters, heat absorption, and acidification dynamics.

Particular attention is given to the role of phytoplankton in global carbon cycling and oxygen production. The analysis indicates that a fraction of anthropogenic CO₂ remains unfixed by photosynthetic processes and contributes to progressive ocean acidification. The results suggest that additional phytoplankton biomass could potentially contribute to partial compensation of excess CO₂ through biological carbon sequestration mechanisms. Estimated cultivation areas represent a relatively small fraction of the total ocean surface, indicating possible applicability of phytoplankton-based mitigation strategies under suitable environmental conditions.

The comparison between calculated and measured pH variations demonstrates satisfactory agreement, with a correlation coefficient of approximately 0.92 and a

root-mean-square error of 0.0023 pH units, which lies within the typical uncertainty range of oceanographic pH measurements. This supports the applicability of the combined thermodynamic model for general estimation of ocean surface state parameters. The suggested relationships between temperature variation, absorbed heat, CO₂ uptake, and pH changes provide a simplified analytical system for investigating interactions between thermal and chemical ocean processes.

The study also has several limitations that should be considered. The suggested model represents a simplified thermodynamic approximation based on globally averaged parameters and does not include regional oceanographic variability, circulation dynamics, biological feedback mechanisms, seasonal fluctuations, or complex carbonate equilibrium processes. Despite of these limitations, the suggested thermodynamic–calorimetric methodology may provide a useful and relatively accessible tool for preliminary assessment of ocean heat uptake, carbon absorption, and acidification trends. The integration of thermodynamic analysis with phytoplankton-related carbon fixation concepts also supports the investigation of nature-based approaches for climate mitigation and environmental monitoring, as well as the validation against recent high-resolution observational datasets.

The suggested method is important because it offers a physical model for the study of complex ocean circulation state. Its practical usefulness lies in the ability to estimate key ocean acidification indicators (pH change, CO₂ uptake, heat absorption) using only routinely measured sea surface temperature data and known CO₂ emission records. This makes the method accessible to research groups for rapid preliminary assessments in data-scarce regions.

The derived analytical expressions can be applied for short- to medium-term forecasting of ocean surface pH trends under different future emission scenarios. By incorporating projected values of atmospheric heat absorption (ΔQ) and CO₂ uptake (Δm(CO₂)), the model can provide first-order predictions of acidification rates, supporting early warning systems for marine ecosystems and informing policy decisions related to carbon mitigation strategies.

In summary, the combined thermodynamic approach provides a physically consistent method for studying the response of ocean surface waters to anthropogenic greenhouse forcing and highlights the potential importance of biological carbon sequestration processes in future climate mitigation strategies.

REFERENCES

- [1] S. A. Henson *et al.*, “Future phytoplankton diversity in a changing climate,” *Nature Communications*, vol. 12, art. no. 4215, 2021. <https://doi.org/10.1038/s41467-021-25699-w>
- [2] J. C. Orr *et al.*, “Anthropogenic ocean acidification over the twenty-first century and its impact on calcifying organisms,” *Nature*, vol. 437, pp. 681–686, 2005. <https://doi.org/10.1038/nature04095>

- [3] V. Silkin *et al.*, “Phytoplankton dynamics and biogeochemistry of the Black Sea,” *Journal of Marine Science and Engineering*, vol. 11, no. 6, art. no. 1196, 2023. <https://doi.org/10.3390/jmse11061196>
- [4] S. I. Anderson *et al.*, “Marine phytoplankton functional types exhibit diverse responses to thermal change,” *Nature Communications*, vol. 12, art. no. 6413, 2021. <https://doi.org/10.1038/s41467-021-26651-8>
- [5] Y. Liu *et al.*, “Global estimates of suitable areas for marine algae farming,” *Environmental Research Letters*, vol. 18, no. 6, art. no. 064028, 2023. <https://doi.org/10.1088/1748-9326/acd3d8>
- [6] B. Midyurova, E. Mollova, and A. Dimitrov, “Adsorption purification technologies for environmental protection applications,” *Oxidation Communications*, vol. 44, no. 2, pp. 412–420, 2021.
- [7] E. Mollova *et al.*, “Investigation of adsorption systems for purification of volatile organic compounds,” *Journal of Environmental Protection and Ecology*, vol. 22, no. 5, pp. 1854–1862, 2021.
- [8] Z. Nikolaeva and D. Ivanova, “Investigation of PM10 concentrations for Burgas municipality,” *Oxidation Communications*, vol. 43, no. 2, pp. 349–356, 2020.
- [9] M. Petrov, “Major contribution of carbon dioxide excess in atmosphere to the greenhouse effect,” *Oxidation Communications*, vol. 44, no. 4, pp. 870–907, 2021.
- [10] D. Ivanova *et al.*, “Study of the concentration of heavy metals in silt loading from transport arteries in the city of Burgas, Bulgaria,” *Oxidation Communications*, vol. 45, no. 2, pp. 390–397, 2022.
- [11] Z. Nikolaeva and I. Parunov, “Assessment of PM10 concentrations and COVID-19 disease for Burgas municipality,” *Oxidation Communications*, vol. 45, no. 2, pp. 383–389, 2022.
- [12] Z. Nikolaeva, “Pollution with PM10 in the atmospheric air and some registered infectious diseases for the municipality of Burgas,” *Oxidation Communications*, vol. 46, no. 3, pp. 747–756, 2023.
- [13] D. Ivanova and Z. Nikolaeva, “Pollution with silt loading on major roads in the city of Burgas, Bulgaria,” *Journal of Environmental Protection and Ecology*, vol. 22, no. 3, pp. 968–975, 2021.
- [14] B. Midyurova and M. D. Todorova, “Ion exchange softening of natural waters of high total hardness,” *Journal of Chemical Technology and Metallurgy*, vol. 56, no. 2, pp. 342–347, 2021.
- [15] B. Midyurova *et al.*, “Performance prediction of a microbial fuel cell based on artificial neural networks,” in *Contemporary Methods in Bioinformatics and Biomedicine and Their Applications*, Lecture Notes in Networks and Systems, vol. 374, Springer, 2022. https://doi.org/10.1007/978-3-030-96638-6_22
- [16] C. M. Domingues *et al.*, “Improved estimates of upper-ocean warming and multi-decadal sea-level rise,” *Nature*, vol. 453, pp. 1090–1093, 2008. <https://doi.org/10.1038/nature07080>
- [17] D. P. Häder and K. Gao, “Interactions of anthropogenic stress factors on marine phytoplankton,” *Frontiers in Environmental Science*, vol. 3, art. no. 14, 2015. <https://doi.org/10.3389/fenvs.2015.00014>
- [18] V. J. Fabry *et al.*, “Impacts of ocean acidification on marine fauna and ecosystem processes,” *ICES Journal of Marine Science*, vol. 65, no. 3, pp. 414–432, 2008. <https://doi.org/10.1093/icesjms/fsn048>
- [19] E. Hristova *et al.*, “Black carbon in Bulgaria—observed and modelled concentrations in two cities for two months,” *Atmosphere*, vol. 13, no. 2, art. no. 213, 2022. <https://doi.org/10.3390/atmos13020213>
- [20] Y. M. Bar-On, R. Phillips, and R. Milo, “The biomass distribution on Earth,” *PNAS*, vol. 115, no. 25, pp. 6506–6511, 2018. <https://doi.org/10.1073/pnas.1711842115>
- [21] M. L. Ghirardi *et al.*, “Microalgae: a green source of renewable H₂,” *Trends in Biotechnology*, vol. 18, no. 12, pp. 506–511, 2000. [https://doi.org/10.1016/S0167-7799\(00\)01511-0](https://doi.org/10.1016/S0167-7799(00)01511-0)
- [22] R. Kutsarov *et al.*, “Research of the air pollution in the town of Burgas (Bulgaria) with BTEX and alkanes,” *Pollution Atmosphérique*, no. 194, 2007.
- [23] J. T. Kiehl and K. E. Trenberth, “Earth’s global energy budget,” *Bull. Amer. Meteorol. Soc.*, vol. 78, no. 2, pp. 197–208, 1997. [https://doi.org/10.1175/1520-0477\(1997\)078<0197:EAGMEB>2.0.CO;2](https://doi.org/10.1175/1520-0477(1997)078<0197:EAGMEB>2.0.CO;2)
- [24] K. E. Trenberth *et al.*, “Earth’s global energy budget,” *Bull. Amer. Meteorol. Soc.*, vol. 90, no. 3, pp. 311–323, 2009. <https://doi.org/10.1175/2008BAMS2634.1>
- [25] S. Levitus *et al.*, “Warming of the world ocean, 1955–2003,” *Geophys. Res. Lett.*, vol. 32, L02604, 2005. <https://doi.org/10.1029/2004GL021592>
- [26] Copernicus Climate Change Service, “Global temperature and CO₂ trends,” 2025. <https://climate.copernicus.eu/last-four-years-have-been-warmest-record-and-co2-continues-rise>
- [27] NASA Earth Observatory, “Global temperatures,” 2025. <https://earthobservatory.nasa.gov/world-of-change/global-temperatures>
- [28] J. J. Cole and Y. T. Prairie, “Dissolved CO₂ in freshwater systems,” in *Encyclopedia of Inland Waters*, Elsevier, 2014. <https://doi.org/10.1016/B978-0-12-409548-9.09399-4>
- [29] R. E. Zeebe and D. A. Wolf-Gladrow, “Carbon dioxide, dissolved (ocean),” in *Encyclopedia of Ocean Sciences*, Springer, 2009. https://doi.org/10.1007/978-1-4020-4411-3_30
- [30] J. Wu *et al.*, “Nearshore macroalgae cultivation for carbon sequestration,” *Geophys. Res. Lett.*, vol. 52, e2025GL116774, 2025. <https://doi.org/10.1029/2025GL116774>
- [31] P. G. Falkowski, “Global biogeochemical cycles,” *Photosynthesis Research*, vol. 39, pp. 235–258, 1994. <https://doi.org/10.1007/BF00014586>
- [32] S. Ozaki, “Global warming mitigation via plankton CO₂ assimilation,” *J. Marine Sci. Res. Dev.*, vol. 6, no. 4, 2016. <https://doi.org/10.4172/2155-9910.1000213>
- [33] C. M. Duarte *et al.*, “Seaweed farming and climate change mitigation,” *Frontiers in Marine Science*, vol. 4, 2017. <https://doi.org/10.3389/fmars.2017.00100>
- [34] A. Gagem and L. Kapsenberg, *Ocean-based carbon dioxide removal*, ClimateWorks Foundation, 2021.
- [35] M. Grégoire *et al.*, *Ocean oxygen and deoxygenation*, European Marine Board, 2023. <https://doi.org/10.5281/zenodo.7941157>
- [36] D. A. Hutchins and F.-X. Fu, “Microorganisms and ocean global change,” *Nature Microbiology*, vol. 2, 2017. <https://doi.org/10.1038/nmicrobiol.2017.58>
- [37] J.-P. Gattuso *et al.*, “Ocean solutions to address climate change,” *Frontiers in Marine Science*, vol. 5, 2018. <https://doi.org/10.3389/fmars.2018.00337>
- [38] L. Delaigue *et al.*, “Surface ocean pH variability,” *Biogeosciences*, vol. 22, pp. 5103–5122, 2025. <https://doi.org/10.5194/bg-22-5103-2025>
- [39] D. C. E. Bakker *et al.*, “Uncertainty in seawater carbonate chemistry observations,” *ESSD*, vol. 16, pp. 4573–4596, 2024. <https://doi.org/10.5194/essd-16-4573-2024>
- [40] P. Friedlingstein *et al.*, “Global Carbon Budget 2025,” *ESSD*, vol. 18, pp. 3211–3299, 2026. <https://doi.org/10.5194/essd-18-3211-2026>
- [41] A. Hogikyan and L. Resplandy, “Hydrological cycle amplification,” *Biogeosciences*, vol. 21, pp. 4621–4639, 2024. <https://doi.org/10.5194/bg-21-4621-2024>
- [42] R. G. J. Bellerby *et al.*, “A new indicator for ocean acidification capacity,” *Commun. Earth Environ.*, vol. 6, 2025. <https://doi.org/10.1038/s43247-025-02380-4>
- [43] S. K. Lauvset *et al.*, “GLODAPv2.2024 data product,” *ESSD*, vol. 16, pp. 1381–1405, 2024. <https://doi.org/10.5194/essd-16-1381-2024>

Competing Thermodynamic and Radiative Effects on Atmospheric Circulation in Polluted Environments

Mihai Petrov

dept. of Natural Sciences

Burgas State University "Pr. Dr. Assen Zlatarov"

Burgas, Bulgaria

mihai-petrov@uniburgas.bg;

ORCID: [0000-0003-0811-1250](https://orcid.org/0000-0003-0811-1250)

Abstract—This study develops a unified method linking thermodynamic processes and radiative feedbacks in a human altered atmosphere, combining an adiabatic calorimetric perspective with a radiation balance model to describe wind changes. Air pollutants produce two competing effects: thermodynamic damping, where polyatomic gases and aerosols modify air properties and reduce wind speed, and radiative effects linked to increased reflectivity that can enhance or stabilize winds. A feedback ratio determines which mechanism dominates. When thermodynamic damping prevails, wind stilling occurs in regions with high absorbing aerosols; when radiative effects dominate, winds remain stable or slightly intensify in scattering aerosol environments. The regime depends strongly on aerosol composition, with scattering particles promoting stability and absorbing particles driving destabilization. These results show that accurate climate projections require considering aerosol composition alongside greenhouse gases, highlighting complex non linear coupling between air quality and atmospheric circulation.

Keywords— *adiabatic constant, damping, pollutants, speed of wind.*

I. INTRODUCTION

Human activity alters the atmosphere through greenhouse gases and aerosols, affecting temperature, pressure, specific heat capacity (c_p), and the adiabatic constant (γ), which control climate dynamics. Radiatively active gases, especially CO_2 and CH_4 , drive warming, with CO_2 contributing about 75% of emissions [1], [2], [3], [4], [5], [6]. Fossil fuel use also reduces O_2 and increases polyatomic gases and aerosols [7], [8]. These changes modify thermodynamic properties: aerosols affect radiation and heat transfer [9], [10], while c_p decreases ($\sim 1010 \rightarrow 992 \text{ J}\cdot\text{kg}^{-1}\cdot\text{K}^{-1}$) and γ ($\sim 1.101 \rightarrow 1.061$) [11], [12], [10], [13], potentially reducing wind speed by up to 20% [14]. Aerosols also alter radiative balance by enhancing

cloud reflectivity (Twomey effect) [15], [16], while land use and black carbon modify albedo [17], [18], [19]. Marine aerosols increase reflectivity, whereas black carbon reduces it and affects circulation [20], [21], [22].

II. MATERIALS AND METHODS

A quantitative description of atmospheric conditions affected by greenhouse pollutants, including the relationship between air temperature and variations in pollutant concentration, was reported in [1].

$$\Delta T = (\gamma - 1) \cdot \frac{\Delta C \cdot T}{C} \quad (1)$$

here, C denotes the overall molar concentration of atmospheric air, while ΔC corresponds to the variation in concentration produced by the presence of greenhouse pollutants, and T represents the atmospheric temperature. Estimated molar concentrations allow evaluation of ΔT from ΔC . Over the past 50 years, global mean temperature has risen approximately linearly [3], mainly driven by CO_2 , which accounts for $\sim 75\%$ of fossil fuel emissions [6], [7]. Since the industrial era, emissions have increased by about 70% (1970–2004) [5]. This warming can be described using thermodynamic and calorimetric approaches [6]. CO_2 growth is also linked to a net O_2 decline due to incomplete photosynthetic compensation [7]. The present study applies a combined adiabatic calorimetric formulation following [6].

$$\Delta T(t) = \frac{\Delta Q(t) + c \cdot (\Delta m(\text{O}_2) - \Delta m(\text{CO}_2)) \cdot (T - T_{\text{eff}})}{c \cdot [m - \Delta m(\text{O}_2) + \Delta m(\text{CO}_2)]} \quad (2)$$

The atmospheric mass is $m \approx 5.13 \times 10^{18} \text{ kg}$ [23], with effective temperature $T_{\text{eff}} = 253 \text{ K}$ and specific heat capacity $c \approx 1007 \text{ J}\cdot\text{kg}^{-1}\cdot\text{K}^{-1}$ [6], [23]. About 60% of excess heat ΔQ is absorbed by the Oceans [24], [25], [26],

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.97>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

which also take up ~30% of atmospheric CO₂ [27], [28], [29], [30], [31]. Accordingly, atmospheric heat and mass terms are written as follows:

$$\Delta m(\text{CO}_2) \rightarrow 0.7 \cdot \Delta m(\text{CO}_2) \Delta Q(t) \rightarrow 0.4 \cdot \Delta Q(t) \quad (3)$$

Therefore (2) incorporating the absorption of both heat and carbon dioxide by the Oceans, can be expressed as:

$$\Delta T(t) = \frac{0.4 \cdot \Delta Q(t) + c \cdot (\Delta m(\text{O}_2) - 0.7 \cdot \Delta m(\text{CO}_2)) \cdot (T - T_{\text{eff}})}{c \cdot [m - \Delta m(\text{O}_2) + 0.7 \cdot \Delta m(\text{CO}_2)]} \quad (4)$$

Since ~60% of heat is absorbed by the Oceans, only ~40% remains in the atmosphere; thus the annual retained heat is $0.4 \times 3.05 \times 10^{20} \text{ J/year} = 1.22 \times 10^{20} \text{ J/year}$. Temperature variations calculated from (4) are shown in the last column of Table 1.

TABLE 1 CALCULATIONS OF THE VARIATION OF ATMOSPHERE'S TEMPERATURE WITH TIME [6]

No	Year	ΔT_r ; (°C)	ΔQ ;(J)	Δm (CO ₂); (kg)	Δm (O ₂); (kg)	ΔT (°C)
0	1980	0	0	0	0	0
1	1981	0.03	$1.22 \cdot 10^{20}$	$1.08 \cdot 10^{13}$	$1.8 \cdot 10^{13}$	0.023
2	1982	0.05	$2.44 \cdot 10^{20}$	$1.62 \cdot 10^{13}$	$1.9 \cdot 10^{13}$	0.047
3	1983	0.07	$3.66 \cdot 10^{20}$	$2.7 \cdot 10^{13}$	$2 \cdot 10^{13}$	0.070
4	1984	0.09	$4.88 \cdot 10^{20}$	$3.78 \cdot 10^{13}$	$2.2 \cdot 10^{13}$	0.094
5	1985	0.11	$6.1 \cdot 10^{20}$	$4.86 \cdot 10^{13}$	$2.3 \cdot 10^{13}$	0.117
6	1986	0.13	$7.32 \cdot 10^{20}$	$5.4 \cdot 10^{13}$	$2.31 \cdot 10^{13}$	0.141
7	1987	0.15	$8.54 \cdot 10^{20}$	$5.94 \cdot 10^{13}$	$2.4 \cdot 10^{13}$	0.165
8	1988	0.18	$9.76 \cdot 10^{20}$	$6.48 \cdot 10^{13}$	$2.42 \cdot 10^{13}$	0.188
9	1989	0.19	$1.1 \cdot 10^{21}$	$6.75 \cdot 10^{13}$	$2.5 \cdot 10^{13}$	0.212
10	1990	0.22	$1.22 \cdot 10^{21}$	$7.02 \cdot 10^{13}$	$2.53 \cdot 10^{13}$	0.235
11	1991	0.26	$1.34 \cdot 10^{21}$	$7.56 \cdot 10^{13}$	$2.56 \cdot 10^{13}$	0.259
12	1992	0.32	$1.46 \cdot 10^{21}$	$8.1 \cdot 10^{13}$	$2.6 \cdot 10^{13}$	0.283
13	1993	0.34	$1.59 \cdot 10^{21}$	$9.18 \cdot 10^{13}$	$2.62 \cdot 10^{13}$	0.306
14	1994	0.36	$1.71 \cdot 10^{21}$	$1.03 \cdot 10^{14}$	$2.71 \cdot 10^{13}$	0.330
15	1995	0.37	$1.83 \cdot 10^{21}$	$1.13 \cdot 10^{14}$	$2.74 \cdot 10^{13}$	0.353
16	1996	0.39	$1.95 \cdot 10^{21}$	$1.19 \cdot 10^{14}$	$2.78 \cdot 10^{13}$	0.377
17	1997	0.41	$2.07 \cdot 10^{21}$	$1.24 \cdot 10^{14}$	$2.8 \cdot 10^{13}$	0.400
18	1998	0.42	$2.2 \cdot 10^{21}$	$1.3 \cdot 10^{14}$	$2.9 \cdot 10^{13}$	0.424
19	1999	0.43	$2.32 \cdot 10^{21}$	$1.35 \cdot 10^{14}$	$3 \cdot 10^{13}$	0.448
20	2000	0.45	$2.44 \cdot 10^{21}$	$1.46 \cdot 10^{14}$	$3.1 \cdot 10^{13}$	0.471
21	2001	0.46	$2.56 \cdot 10^{21}$	$1.67 \cdot 10^{14}$	$3.12 \cdot 10^{13}$	0.495
22	2002	0.47	$2.68 \cdot 10^{21}$	$1.89 \cdot 10^{14}$	$3.2 \cdot 10^{13}$	0.518
23	2003	0.5	$2.81 \cdot 10^{21}$	$2 \cdot 10^{14}$	$3.3 \cdot 10^{13}$	0.542
24	2004	0.54	$2.93 \cdot 10^{21}$	$2.05 \cdot 10^{14}$	$3.4 \cdot 10^{13}$	0.565
25	2005	0.58	$3.05 \cdot 10^{21}$	$2.16 \cdot 10^{14}$	$3.43 \cdot 10^{13}$	0.589
26	2006	0.59	$3.17 \cdot 10^{21}$	$2.22 \cdot 10^{14}$	$3.5 \cdot 10^{13}$	0.612
27	2007	0.6	$3.29 \cdot 10^{21}$	$2.27 \cdot 10^{14}$	$3.55 \cdot 10^{13}$	0.636
28	2008	0.61	$3.42 \cdot 10^{21}$	$2.32 \cdot 10^{14}$	$3.6 \cdot 10^{13}$	0.659
29	2009	0.62	$3.54 \cdot 10^{21}$	$2.38 \cdot 10^{14}$	$3.7 \cdot 10^{13}$	0.683
30	2010	0.63	$3.66 \cdot 10^{21}$	$2.43 \cdot 10^{14}$	$3.8 \cdot 10^{13}$	0.707
31	2011	0.65	$3.78 \cdot 10^{21}$	$2.54 \cdot 10^{14}$	$3.81 \cdot 10^{13}$	0.730
32	2012	0.68	$3.9 \cdot 10^{21}$	$2.97 \cdot 10^{14}$	$3.9 \cdot 10^{13}$	0.754
33	2013	0.7	$4.03 \cdot 10^{21}$	$3.24 \cdot 10^{14}$	$3.94 \cdot 10^{13}$	0.777
34	2014	0.74	$4.15 \cdot 10^{21}$	$3.4 \cdot 10^{14}$	$3.9 \cdot 10^{13}$	0.800
35	2015	0.78	$4.27 \cdot 10^{21}$	$3.46 \cdot 10^{14}$	$3.98 \cdot 10^{13}$	0.824

36	2016	0.8	$4.39 \cdot 10^{21}$	$3.67 \cdot 10^{14}$	$4 \cdot 10^{13}$	0.848
37	2017	0.81	$4.51 \cdot 10^{21}$	$3.89 \cdot 10^{14}$	$4.1 \cdot 10^{13}$	0.871
38	2018	0.82	$4.64 \cdot 10^{21}$	$4 \cdot 10^{14}$	$4.11 \cdot 10^{13}$	0.895
39	2019	0.83	$4.76 \cdot 10^{21}$	$4.05 \cdot 10^{14}$	$4.2 \cdot 10^{13}$	0.918
40	2020	0.85	$4.88 \cdot 10^{21}$	$4.16 \cdot 10^{14}$	$4.22 \cdot 10^{13}$	0.942

The accumulation of anthropogenic heat in the atmosphere, ΔQ , can be expressed in terms of the corresponding variation in atmospheric temperature, ΔT , as indicated by empirical observations, as follows:

$$\Delta Q_{\text{emp}} = c \cdot m_{\text{atm}} \cdot \Delta T_r \quad (5)$$

where m_{atm} is the mass of atmosphere; ΔT_r are the real registered values of the variations of the temperature; c - specific heat capacity of atmospheric air. The combination of the adiabatic method, expressed by (1), and the thermodynamic method, described by (5), allows the formulation of a more general expression that incorporates additional parameters:

$$\Delta Q_{\text{emp}} = (\gamma - 1) \cdot c \cdot m_{\text{atm}} \cdot \frac{T}{C} \cdot \Delta C \quad (6)$$

here, T represents the current average global atmospheric temperature, C is the total molar concentration of the atmosphere, and ΔC denotes the concentration change caused by greenhouse gas accumulation. The specific heat capacity at constant pressure (c_p) is the energy needed to raise a unit mass of gas by one degree and is a mass weighted average in mixtures [11]. The atmosphere is mainly N₂ and O₂, with smaller amounts of Ar and greenhouse gases (CO₂, CH₄), whose molecular properties affect heat capacity [11], [32]. Increasing their concentration can reduce specific heat capacity at constant pressure - c_p [32], [33]. Lower c_p reduces warming energy and increases the dry adiabatic lapse rate dT/dz , affecting stability and convection [34], [35], [36].

$$\frac{dT}{dz} = - \frac{g}{c_p} \quad (7)$$

Here, dT/dz is the temperature gradient, z is altitude, $g = 9.83 \text{ m/s}^2$, and c_p is the specific heat capacity. Rising air cools adiabatically [25], and higher lapse rates increase instability, convection, and extreme weather [36], [37]. Small gradient changes under high greenhouse gas levels can intensify storms, while γ variations are smaller than c_p effects [38], [39]. Albedo controls radiation balance [40], [41]. Scattering aerosols increase reflectivity, while black carbon reduces it and warms the atmosphere [42], [43]. Aerosols also enhance cloud brightness, affecting radiation, microclimate, and circulation [44], [45], [46], [47], [48], [49].

The application of (4) gives possibility to obtain an expression for the specific heat capacity that is written as follows:

$$c = \frac{\Delta Q}{(m - \Delta m(O_2) + \Delta m(CO_2)) \cdot \Delta T - (\Delta m(O_2) - \Delta m(CO_2)) \cdot (T - T_{eff})} = \frac{\Delta Q}{Z} \quad (8)$$

where Z is the expression of denominator from the left side of (8).

Atmospheric air mass dynamics are governed by a complex synergy of factors defined by numerous physicochemical parameters. A primary phenomenon associated with these displacements is wind, which represents the vector quantity of air motion. Wind velocity and flow patterns are subject to modulation by atmospheric constituents, including anthropogenic or natural aerosols and greenhouse gases, which alter the thermal and barometric gradients within the troposphere.

To characterize the vertical transport of air masses under varying thermodynamic conditions, the velocity of ascending air currents is evaluated using the following expression [50], [51]:

$$u = g \cdot h \cdot \sqrt{\frac{2}{c_p \cdot T}} \quad (9)$$

where c_p is the specific heat capacity at constant pressure, T is the atmospheric air temperature, g is the gravitational acceleration, and h denotes altitude. This relationship shows that vertical wind speed depends on atmospheric height, temperature, and the molecular properties of the air mixture. The specific heat capacity at constant pressure (c_p) is given as follows [50], [52], [53]:

$$c_p = \frac{\gamma \cdot R}{\gamma - 1} \quad (10)$$

where R is the universal gas constant and γ is the adiabatic constant of the atmosphere. Substituting (10) into (9) yields the following result:

$$u = g \cdot h \cdot \sqrt{\frac{2}{C_p \cdot T}} = gh \cdot \sqrt{\frac{2}{R}} \cdot \sqrt{\frac{\gamma - 1}{\gamma \cdot T}} \quad (11)$$

The aim is to derive an expression for wind speed variation (Δu) as a function of changes in the adiabatic constant ($\Delta \gamma$), temperature (ΔT), and specific heat capacity (Δc_p). From (11) the following formal operation is obtained:

$$u^2 = \frac{g^2 \cdot h^2 \cdot \sqrt{4 \cdot (\gamma - 1)}}{\sqrt{\gamma \cdot c_p \cdot R \cdot T^2}} = \frac{2 \cdot g^2 \cdot h^2 \cdot \sqrt{\gamma - 1}}{T \cdot \sqrt{\gamma \cdot R \cdot c_p}} \quad (12)$$

Differentiation of (12) makes it possible to obtain an expression that relates the variation of wind speed (Δu) to the proper value of speed u .

$$2 \cdot u \cdot \Delta u = \frac{2 \cdot g^2 \cdot h^2}{\sqrt{R}} \cdot \left(\sqrt{\frac{\gamma - 1}{\gamma \cdot c_p \cdot T^2}} \right)' \quad (13)$$

The derivative of the term $\left(\sqrt{\frac{\gamma - 1}{\gamma \cdot c_p \cdot T^2}} \right)'$ can be examined

under conditions where two consecutive parameters are held constant while the third varies ($\gamma = \text{const}$ or $T = \text{const}$ or $c_p = \text{const}$).

$$\left(\sqrt{\frac{\gamma - 1}{\gamma \cdot c_p \cdot T^2}} \right)'_{\gamma \neq \text{const}} = \frac{1}{2 \cdot \sqrt{c_p \cdot T^2}} \cdot \sqrt{\frac{\gamma}{\gamma - 1}} \cdot \frac{\Delta \gamma}{\gamma^2}; \quad (14)$$

$$\left(\sqrt{\frac{\gamma - 1}{\gamma \cdot c_p \cdot T^2}} \right)'_{T \neq \text{const}} = -\sqrt{\frac{\gamma - 1}{\gamma \cdot c_p}} \cdot \frac{\Delta T}{T^2}; \quad (15)$$

$$\left(\sqrt{\frac{\gamma - 1}{\gamma \cdot c_p \cdot T^2}} \right)'_{c_p \neq \text{const}} = -\frac{1}{2} \cdot \sqrt{\frac{\gamma - 1}{\gamma}} \cdot \frac{\Delta c_p}{c_p \cdot \sqrt{c_p}}; \quad (16)$$

Taking into account (14), (15), and (16), then (13) can be written as follows:

$$u \cdot \Delta u = \frac{g^2 \cdot h^2}{\sqrt{R}} \cdot \left(\frac{1}{2 \cdot T \cdot \sqrt{c_p}} \cdot \sqrt{\frac{\gamma}{\gamma - 1}} \cdot \frac{\Delta \gamma}{\gamma^2} - \sqrt{\frac{\gamma - 1}{\gamma \cdot c_p}} \cdot \frac{\Delta T}{T^2} - \frac{1}{2} \cdot \sqrt{\frac{\gamma - 1}{\gamma \cdot T^2}} \cdot \frac{\Delta c_p}{c_p \cdot \sqrt{c_p}} \right) \quad (17)$$

Then, (11) can be written as follows:

$$g^2 \cdot h^2 = \frac{u^2 \cdot c_p \cdot T}{2} \quad (18)$$

Substituting (18) into (17) yields the following result:

$$\frac{\Delta u}{u} = \frac{c_p \cdot T}{\sqrt{R}} \cdot \left(\frac{1}{2 \cdot T \cdot \sqrt{c_p}} \cdot \sqrt{\frac{\gamma}{\gamma - 1}} \cdot \frac{\Delta \gamma}{\gamma^2} - \sqrt{\frac{\gamma - 1}{\gamma \cdot c_p}} \cdot \frac{\Delta T}{T^2} - \frac{1}{2} \cdot \sqrt{\frac{\gamma - 1}{\gamma \cdot T^2}} \cdot \frac{\Delta c_p}{c_p \cdot \sqrt{c_p}} \right) \quad (19)$$

$$\frac{\Delta u}{u} = \frac{c_p \cdot T}{\sqrt{R}} \cdot \sqrt{\frac{\gamma}{(\gamma - 1) \cdot c_p}} \cdot \left(\frac{1}{2 \cdot T} \cdot \frac{\Delta \gamma}{\gamma^2} - \left(\frac{\gamma - 1}{\gamma} \right) \frac{\Delta T}{T^2} - \frac{\gamma - 1}{2 \cdot \gamma \cdot T} \cdot \frac{\Delta c_p}{c_p} \right) \quad (20)$$

Thus, the expression for the relative change in wind speed $\Delta u/u$ is a multivariable function that depends on the differentials of the adiabatic constant ($\Delta \gamma$), absolute temperature (ΔT), and specific heat capacity at constant pressure (Δc_p). This formulation makes it possible to assess how localized perturbations in thermal properties and gas constants propagate as variations in wind kinetic behavior. By isolating the terms associated with $\Delta \gamma$, ΔT , and Δc_p , the model can identify the relative contribution of each thermodynamic parameter to the overall instability of the velocity field.

The albedo of biosphere components is influenced by temperature changes caused by the presence of pollutant aerosols in the atmosphere. It plays an important role in the formation of the local microclimate. An increase in global temperature leads to a corresponding increase in albedo [48]. The variation of albedo is written as follows [48]:

$$\Delta A = \frac{16 \cdot \varepsilon \cdot \sigma}{I_{sc}} \cdot T_{eff}^3 \cdot \left(\frac{1}{m \cdot c} \cdot \left(\Delta Q - \frac{Q \cdot \Delta m}{m} \right) - \Delta T \right) \quad (21)$$

Pollutants affect both heat trapping and air motion, while albedo further modifies the local microclimate. The value of ΔT , expressed as a function of albedo change (ΔA), can be substituted into (21), yielding the following expression for $\Delta u/u$:

$$\frac{\Delta u}{u} = \frac{\gamma}{(\gamma-1) \cdot \sqrt{R}} \cdot \left[\frac{\Delta \gamma}{2 \cdot \gamma^2} - \frac{(\gamma-1) \cdot T}{\gamma} \cdot \frac{\Delta c_p}{2 \cdot c_p} - \frac{(\gamma-1)}{\gamma \cdot T} \cdot \left(\frac{\Delta Q}{m \cdot c} - \frac{Q \cdot \Delta m}{m^2 \cdot c} \right) + \frac{(\gamma-1)}{\gamma \cdot T} \cdot \frac{\Delta A}{K} \right] \quad (22)$$

where : $K = \frac{16 \cdot \varepsilon \cdot \sigma}{I_{sc}} \cdot T_{eff}^3$; $T_{eff} = T - \frac{Q}{m \cdot c}$

The final expression shows that wind speed depends on both thermodynamic and radiative processes in the atmosphere. Changes in the adiabatic constant, specific heat capacity, and temperature would affect air stability and wind circulation. Higher pollutant concentrations

could decrease the adiabatic constant and suppress normal adiabatic cooling, leading to weaker wind development. Pollutants such as PM2.5, PM10, black carbon, and greenhouse gases would contribute to this thermodynamic damping. In contrast, scattering aerosols increase albedo and could partly compensate for wind reduction by reflecting more solar radiation. Thus, wind behavior is controlled by the balance between thermodynamic damping and albedo-driven stabilization.

III. RESULTS AND DISCUSSION

To evaluate the reliability of the obtained results through comparison with empirical atmospheric data, the proposed calorimetric approach was utilized to recalculate the atmospheric specific heat capacity. Using the formula defined in (8) for specific heat capacity values, the calculated results are presented in Table 2.

TABLE 2 THE DYNAMICS OF VARIATIONS IN ATMOSPHERIC OXYGEN AND CARBON DIOXIDE CONCENTRATIONS [6]

Year	ΔT_r ; °C	$\Delta m(\text{CO}_2)$ $\times 10^{13}$; (kg)	$\Delta m(\text{O}_2)$ $\times 10^{13}$; (kg)	$m \times 10^{18}$; (kg)	$m \times \Delta T_r$; $\times 10^{18}$	$Z \times 10^{18}$	$\Delta Q \times 10^{20}$; (J)
1981	0.03	1.08	1.8	5.49999	0.165	0.164752	1.22
1982	0.05	1.62	1.9	5.5000	0.275	0.274924	2.44
1983	0.07	2.7	2	5.50001	0.385	0.385232	3.66
1984	0.09	3.78	2.2	5.50002	0.495001	0.495523	4.88
1985	0.11	4.86	2.3	5.50003	0.605003	0.605848	6.1
1986	0.13	5.4	2.31	5.50003	0.715004	0.716021	7.32
1987	0.15	5.94	2.4	5.50004	0.825005	0.826181	8.54
1988	0.18	6.48	2.42	5.50004	0.990007	0.991348	9.76
1989	0.19	6.75	2.5	5.50004	1.04501	1.04642	11
1990	0.22	7.02	2.53	5.50005	1.21001	1.21150	12.2
1991	0.26	7.56	2.56	5.50005	1.43001	1.43167	13.4
1992	0.32	8.1	2.6	5.50006	1.76002	1.76184	14.6
1993	0.34	9.18	2.62	5.50007	1.87002	1.87219	15.9
1994	0.36	10.3	2.71	5.50008	1.98003	1.98253	17.1
1995	0.37	11.3	2.74	5.50009	2.03503	2.03789	18.3
1996	0.39	11.9	2.78	5.50009	2.14504	2.14806	19.5
1997	0.41	12.4	2.8	5.5001	2.25504	2.25821	20.7
1998	0.42	13	2.9	5.5001	2.31004	2.31355	22
1999	0.43	13.5	3	5.50011	2.36505	2.36852	23.2
2000	0.45	14.6	3.1	5.50012	2.47505	2.47888	24.4
2001	0.46	16.7	3.12	5.50014	2.53060	2.53457	25.6
2002	0.47	18.9	3.2	5.50016	2.58507	2.59026	26.8
2003	0.5	20	3.3	5.50017	2.75008	2.75338	28.1
2004	0.54	20.5	3.4	5.50017	2.97009	2.97576	29.3
2005	0.58	21.6	3.43	5.50018	3.19011	3.19612	30.5
2006	0.59	22.2	3.5	5.50019	3.24511	3.25128	31.7
2007	0.6	22.7	3.55	5.50019	3.30022	3.30644	32.9
2008	0.61	23.2	3.6	5.50020	3.35512	3.36160	34.2

2009	0.62	23.8	3.7	5.50020	3.41012	3.41674	35.4
2010	0.63	24.3	3.8	5.50021	3.46513	3.47190	36.6
2011	0.65	25.4	3.81	5.50022	3.57514	3.58225	37.8
2012	0.68	29.7	3.9	5.50026	3.74018	3.74871	39
2013	0.7	32.4	3.94	5.50029	3.85020	3.85962	40.3
2014	0.74	34	3.97	5.50030	4.07022	4.08017	41.5
2015	0.78	34.6	3.98	5.50031	4.29024	4.30036	42.7
2016	0.8	36.7	4	5.50033	4.40026	4.41108	43.9
2017	0.81	38.9	4.1	5.50035	4.45528	4.4660	45.1
2018	0.82	40	4.11	5.50036	4.51029	4.5220	46.4
2019	0.83	40.5	4.2	5.50036	4.56530	4.5700	47.6
2020	0.85	41.6	4.22	5.50037	4.67532	4.6870	48.8

The specific heat capacity c can be determined graphically from $\Delta Q = f(Z)$, where it corresponds to the slope of the linear dependence in Fig. 1. The value of Z is calculated from experimentally measured atmospheric temperature variations ΔT_r . The value of c is obtained from the slope of the first linear segment of the graph in Fig. 1.

$$c = \text{tg} \alpha = \frac{\Delta(\Delta Q)}{\Delta Z} = \frac{1,01 \cdot 10^{21}}{1 \cdot 10^{18}} \approx 1010 \left(\frac{J}{kg \cdot K} \right) \quad (23)$$

The dependence of ΔQ shows a smaller slope in the second linear segment as temperature and Z increase. This behavior suggests that the effective specific heat capacity decreases with higher concentrations of atmospheric pollutants. Since the slope of the linear relation corresponds to the specific heat capacity $c = \Delta Q / (m \cdot \Delta T)$, a smaller slope indicates a lower value of c . Therefore, the second linear segment gives:

$$c = \text{tg} \alpha = \frac{\Delta(\Delta Q)}{\Delta Z} = \frac{(4,5 - 1,01) \cdot 10^{21}}{(4,5 - 1) \cdot 10^{18}} \approx 997 \left(\frac{J}{kg \cdot K} \right) \quad (24)$$

The analysis shows that accumulated atmospheric heat can be described by a semiempirical relation based on thermodynamic calorimetric principles. The excess heat ΔQ depends linearly on atmospheric temperature variation, where m_{atm} (Table 2) is the atmospheric mass and ΔT_r represents measured temperature changes. This linearity is shown in Fig. 2. The specific heat capacity is determined from the slope of the first linear segment.

$$\text{tg} \alpha = \frac{1,05 \cdot 10^{21}}{0,19} = 5,52 \cdot 10^{21} \quad (25)$$

$$c = \frac{\text{tg} \alpha}{m_{\text{atm}}} = \frac{5,52 \cdot 10^{21}}{5,5 \cdot 10^{18}} \approx 1004 \left(\frac{J}{kg \cdot K} \right) \quad (26)$$

The second linear segment of Fig. 2 yields the following relationship:

$$\text{tg} \alpha = c \cdot m_{\text{atm}} = \frac{(4,68 - 1,05) \cdot 10^{21}}{(0,855 - 0,19)} = 5,458 \cdot 10^{21}$$

$$(27) \quad c = \frac{5,458 \cdot 10^{21}}{5,5 \cdot 10^{18}} \approx 992 \left(\frac{J}{kg \cdot K} \right)$$

$$(28)$$

The corresponding dependence $\Delta Q = f(m_{\text{atm}} \cdot \Delta T_r)$ is illustrated in Fig. 3. The specific heat capacity, c , can also be determined from the slope of the linear segments. Two distinct segments are observed in Fig. 3. The first segment yields:

$$c = \text{tg} \alpha = \frac{\Delta(\Delta Q)}{\Delta(m_{\text{atm}} \cdot \Delta T_r)} = \frac{1,01 \cdot 10^{21}}{1 \cdot 10^{18}} \approx 1010 \left(\frac{J}{kg \cdot K} \right) \quad (29)$$

The second segment yields:

$$c = \text{tg} \alpha = \frac{\Delta(\Delta Q)}{\Delta(m_{\text{atm}} \cdot \Delta T_r)} = \frac{(4,69 - 1,01) \cdot 10^{21}}{(4,71 - 1) \cdot 10^{18}} \approx 992 \left(\frac{J}{kg \cdot K} \right) \quad (30)$$

The evaluation of the specific heat capacity of atmospheric air is essential because it strongly affects the thermodynamic state of the atmosphere. Atmospheric temperature depends mainly on air composition and specific heat capacity.

Analysis of O_2 and CO_2 trends shows that CO_2 accumulation increases atmospheric mass [30], [31]. Higher greenhouse gas levels reduce specific heat capacity, while greater mass raises density and pressure [54], [55]. Since higher density is linked to lower heat capacity [56], the relation $\Delta Q = f(m_{\text{atm}} \cdot \Delta C)$ (Fig. 4) allows estimation of γ , which decreases as pollutants increase.

$$\text{tg} \alpha = \frac{(\gamma - 1) \cdot c \cdot T}{C} = \frac{(24,1 - 0) \cdot 10^{20}}{(34 - 0) \cdot 10^{14}} = 0,7088 \cdot 10^6 \quad (31)$$

The overall average molar concentration of the atmosphere is $C = 0,04137 \text{ mol/l}$. Using this value, the corresponding parameters in the previously derived expressions can be calculated to quantify the specific heat capacity and the adiabatic constant of atmospheric air under the given conditions.

$$\frac{(\gamma - 1) \cdot c \cdot T}{C} = 0,7088 \cdot 10^6; \quad (\gamma - 1) = \frac{0,7088 \cdot 10^6 \cdot C}{c \cdot T} \quad (32)$$

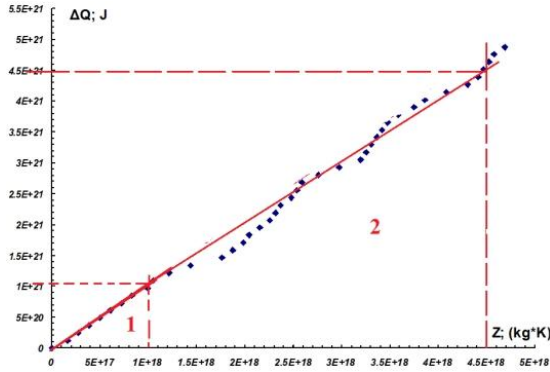


Fig. 1. Calculation of the Specific Heat Capacity of Atmospheric Air Based on Excess Atmospheric Heat (ΔQ).

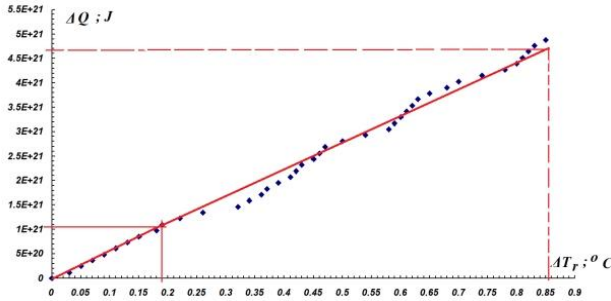


Fig. 2. Atmospheric excess heat variations as a function of temperature change.

For the first segment of Fig. 4, the specific heat capacity of the atmosphere is $c=1007 \text{ J/(kg} \cdot \text{K)}$ and the temperature is $T \approx 288 \text{ K}$. Using these values, the adiabatic constant γ can be calculated as follows:

$$\gamma = 1 + \frac{0.7088 \cdot 10^6 \cdot C}{c \cdot T} = 1.101 \quad (33)$$

The second segment exhibits the following slope:

$$\text{tg} \alpha = \frac{(\gamma - 1) \cdot c \cdot T}{C} = \frac{(50.4 - 24.1) \cdot 10^{20}}{(96 - 34) \cdot 10^{14}} = 0.42419 \cdot 10^6 \quad (34)$$

For the second segment of Fig. 4, the specific heat capacity of the atmosphere is $c = 992 \text{ J/(kg} \cdot \text{K)}$ and the temperature is approximately $T \approx 288 \text{ K}$. Using these values, the corresponding adiabatic constant γ can be calculated as follows:

$$\gamma = 1 + \frac{0.42419 \cdot 10^6 \cdot C}{c \cdot T} = 1 + \frac{0.42419 \cdot 10^6 \cdot 0.04137}{992 \cdot 288} = 1.061 \quad (35)$$

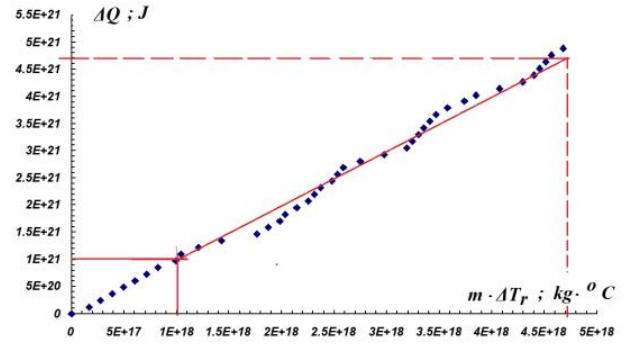


Fig. 3. Changes in atmospheric excess heat as a function of $m_{\text{atm}} \cdot \Delta T_r$.

Increasing atmospheric pollution decreases the adiabatic constant γ [57]. In clean air dominated by N_2 and O_2 , γ is about 1.4 [50], while lower values (1.101–1.061) indicate higher levels of polyatomic gases and pollutants [58]. These molecules increase heat capacity and reduce γ [59]. The decrease in specific heat to about $992 \text{ J} \cdot \text{kg}^{-1} \cdot \text{K}^{-1}$ affects adiabatic processes, vertical motion, and cloud formation [60]. Since $\gamma = 1 + 2/f$, the low value $\gamma \approx 1.106$ reflects molecular complexity, aerosols, and humidity [10], [13], [57], [58], [60], [61], [62], [63].

Fig. 4 shows that for higher pollutant levels γ is reduced, weakened adiabatic cooling during ascent, and increase buoyancy, instability, storm intensity, and cloud formation. Values are summarized in Table 4 [10], [57], [58], [60], [61], [62].

Atmospheric stability and wind dynamics depend on the thermodynamic properties of air parcels [64]. Pressure gradients drive wind, while polyatomic pollutants lower γ and increase instability [58]. Reduced γ (1.101 → 1.061) causes greater energy storage in molecular modes [10], stronger turbulence and lower predictability [65], slower cooling with $c_p \approx 992 \text{ J} \cdot \text{kg}^{-1} \cdot \text{K}^{-1}$, and enhanced vertical wind shear and updrafts [65]. These effects are summarized in Table 5 [10], [57], [58], [60], [61], [62].

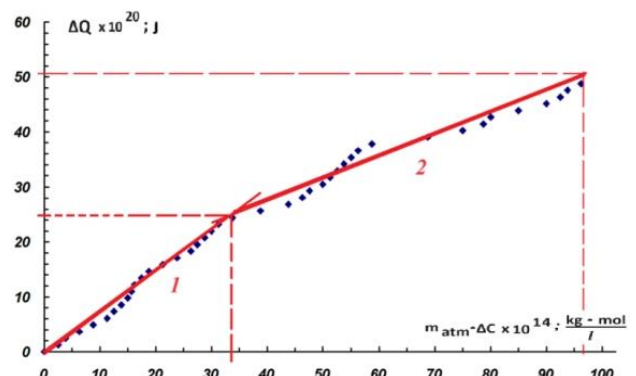


Fig. 4. Graphical dependence of $\Delta Q = f(m_{\text{atm}} \cdot \Delta C)$.

TABLE 3 VALUES OF ADIABATIC CONSTANT AS THE FUNCTION OF QUANTITY OF MODES F [10], [62], [63]

Category	Pollutant	γ	f	Conc. (mol/L)	Conc. (g/l)
Clean Air	Nitrogen / Oxygen N ₂ /O ₂	1.40	5	4.1×10^{-2}	1.2
Greenhouse Gases	Carbon Dioxide CO ₂	1.30	7	1.7×10^{-5}	7.5×10^{-4}
	Methane CH ₄	1.32	6	8.2×10^{-8}	1.3×10^{-6}
	Nitrous Oxide N ₂ O	1.31	7	1.4×10^{-8}	6.2×10^{-7}
	Ozone O ₃	1.29	7	2.0×10^{-9}	9.6×10^{-8}
	Sulfur Hexafluori de SF ₆	1.09	2 2	4.0×10^{-13}	5.8×10^{-11}
Acid Rain/Industri al	Sulfur Dioxide SO ₂	1.29	6	4.0×10^{-10}	2.6×10^{-8}
	Nitrogen Dioxide NO ₂	1.33	6	8.0×10^{-10}	3.7×10^{-8}
VOCs (Aromatics)	Toluene C ₇ H ₈	1.07	2 8	1.1×10^{-9}	1.0×10^{-7}
	Benzene C ₆ H ₆	1.10	2 0	6.4×10^{-10}	5.0×10^{-8}
Particulates	PM _{2.5} Aerosol	1.06	3 3	—	1.5×10^{-7}
	PM ₁₀ Aerosol	1.04	5 0	—	4.5×10^{-7}

TABLE 4 THERMODYNAMIC VARIATIONS IN ATMOSPHERIC DEGREES OF FREEDOM AND SPECIFIC HEAT AS A FUNCTION OF POLLUTANT CONCENTRATION [10], [57], [58], [60], [61], [62]

Feature	Segment 1 (Less Polluted)	Segment 2 (More Polluted)
Adiabatic Constant γ	1.101	1.061
Specific Heat (c)	1007 J/(kg K)	992 J/(kg K)
Degrees of Freedom (f)	≈ 20	≈ 33
Cooling Profile	Rapid cooling as it rises.	Slower cooling; retains heat longer.

TABLE 5 THERMODYNAMIC MODULATION OF WIND DYNAMICS AND ATMOSPHERIC STABILITY [10], [57], [58], [60], [61], [62]

Metric	High γ (Segment 1)	Low γ (Segment 2 – more Polluted)
Adiabatic Constant	1.101	1.061
Air Response	Sharp pressure changes.	High energy absorption/damping.
Horizontal Wind	Faster propagation of pressure waves.	Potentially more stagnant or turbulent.
Vertical Wind	Standard cooling; stable.	Slower cooling; high buoyancy/instability.

The last part of (20), involving ΔT , $\Delta \gamma$, and Δc_p , shows that increasing temperature ($\Delta T > 0$) generally reduces specific heat capacity ($\Delta c_p < 0$) [66]. The adiabatic constant $\gamma = c_p/c_v$ controls adiabatic processes and supports wind formation through buoyancy [67], [68]. A reduction in γ due to PM_{2.5}/PM₁₀ lowers atmospheric stability and suppresses wind development [69]. When γ decreases while T and c_p remain constant, wind speed slightly decreases. The effects are summarized in Table 6 [70], [71].

TABLE 6 EFFECT OF THERMODYNAMIC PARAMETERS ON WIND SPEED [70], [71]

Temp-re; (T)	Specific heat capacity; (C _p)	Adiabatical constant - γ	Wind speed effect
increasing	decreasing	constant	Faster increase
increasing	decreasing	decreasing	Slower increase
constant	constant	decreasing	Slight decrease / lower acceleration

Fig. 5 shows thermodynamic damping of wind velocity due to polyatomic pollutants. The red curve ($\gamma = \text{const}$) represents the standard adiabatic case, where rising temperature enhances wind acceleration ($\Delta u/u$) through buoyancy and the dry adiabatic lapse rate [65], [72]. The blue curve (γ decreasing) represents a polluted atmosphere with aerosols (PM_{2.5}, PM₁₀), where increased molecular degrees of freedom reduce γ and suppress wind acceleration by lowering instability [58], [60].

The calculation of first term of (20) yields:

$$\frac{c_p \cdot T}{\sqrt{R}} \cdot \frac{\gamma}{\sqrt{(\gamma-1) \cdot c_p}} = \frac{1007 \cdot 288}{\sqrt{8.31}} \cdot \frac{1.4}{\sqrt{0.4 \cdot 1007}} = 5.8 \cdot 10^3 \quad (36)$$

The following cases are examined:

1) $\Delta T \neq 0$; $\Delta c_p \neq 0$; $\Delta \gamma \neq 0$

The variations of temperature $\Delta T \approx 1(\text{K})$; $\Delta c_p \approx -10$ (J/(kg.K)); $\Delta \gamma \approx -0.04$

$$\left(\frac{1}{2T} \cdot \frac{\Delta\gamma}{\gamma^2} - \left(\frac{\gamma-1}{\gamma} \right) \frac{\Delta T}{T^2} - \frac{\gamma-1}{2 \cdot \gamma \cdot T} \cdot \frac{\Delta c_p}{c_p} \right) =$$

$$= \frac{1}{2 \cdot 288} \cdot \left(\frac{-0.04}{1.4^2} \right) - \frac{0.4}{1.4} \cdot \frac{1}{288^2} - \frac{0.4}{2 \cdot 1.4 \cdot 288} \cdot \left(\frac{-10}{1007} \right) = -33.95 \cdot 10^{-6}$$

(37)

$$\frac{\Delta u}{u} = 5.8 \cdot 10^3 \cdot (-33.95) \cdot 10^{-6} = -0.1961$$
(38)

Sometimes the speed of wind is intensified and sometimes is damped drastically. For this case, there is a case of damping of the speed of wind ($\approx -20\%$).

2) $\Delta T \neq 0$; $\Delta c_p \neq 0$; $\Delta\gamma = 0$

The variations of temperature $\Delta T \approx 1(K)$; $\Delta c_p \approx -10 (J/(kg \cdot K))$; $\Delta\gamma = 0$

The case when the adiabatic constant is non-changeable ($\gamma = \text{const}$), then $\Delta\gamma = 0$ and the calculations give

$$\left(\frac{1}{2T} \cdot \frac{\Delta\gamma}{\gamma^2} - \left(\frac{\gamma-1}{\gamma} \right) \frac{\Delta T}{T^2} - \frac{\gamma-1}{2 \cdot \gamma \cdot T} \cdot \frac{\Delta c_p}{c_p} \right) =$$

$$= 0 - \frac{0.4}{1.4} \cdot \frac{1}{288^2} - \frac{0.4}{2 \cdot 1.4 \cdot 288} \cdot \left(\frac{-10}{1007} \right) = 1.48 \cdot 10^{-6}$$
(39)

$$\frac{\Delta u}{u} = 5.8 \cdot 10^3 \cdot 1.48 \cdot 10^{-6} = 0.0086$$
(40)

For this case the speed of wind is intensified (is increased) by $\approx 0.86\%$

3) $\Delta T = 0$; $\Delta c_p = 0$; $\Delta\gamma \neq 0$

The variations of temperature $\Delta T = 0$; $\Delta c_p = 0$; $\Delta\gamma \approx -0.04$

$$\left(\frac{1}{2T} \cdot \frac{\Delta\gamma}{\gamma^2} - \left(\frac{\gamma-1}{\gamma} \right) \frac{\Delta T}{T^2} - \frac{\gamma-1}{2 \cdot \gamma \cdot T} \cdot \frac{\Delta c_p}{c_p} \right) =$$

$$= \frac{1}{2 \cdot 288} \cdot \left(\frac{-0.04}{1.4^2} \right) - 0 - 0 = -3.543 \cdot 10^{-5}$$
(41)

$$\frac{\Delta u}{u} = 5.8 \cdot 10^3 \cdot (-3.543) \cdot 10^{-5} = -0.205$$
(42)

Wind speed decreases by about 21%. Pollutants reduce wind through thermodynamic damping and aerosol-meteorology feedback [73], [74], [75], [76]. PM2.5, PM10, and black carbon act through radiative forcing, atmospheric stabilization, and thermodynamic damping, where higher molecular complexity raises c_p and lowers γ , reducing wind speed [77], [78], [73], [75], [79], [80], [81], [82], [76], [83], [84]. Studies show strong negative correlations ($r \approx -0.8$) between pollution and wind speed [81], [82], with long-term aerosol-driven terrestrial stilling [73], [78].

Since the values of albedo increase with time ($\Delta A > 0$) [48], the change in wind speed obtained from (27) may become positive, which indicates an increase in wind speed ($\Delta u > 0$). The contributions to the change of speed are presented in Table 7.

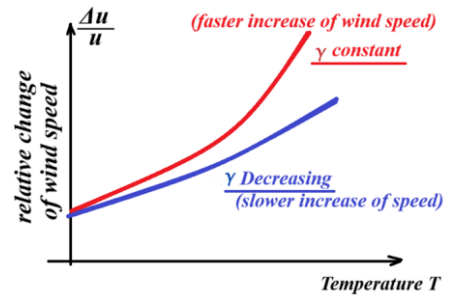


Fig. 5. Thermodynamic Damping of Wind Velocity by Polyatomic Pollutants.[43-45]

TABLE 7 INFLUENCE OF THERMODYNAMIC AND ALBEDO FEEDBACK TERMS ON WIND VELOCITY

Contribution	Sign	Effect on Wind
Direct thermodynamic terms ($\Delta\gamma, \Delta c_p$)	Negative	Decrease wind
Albedo feedback term (ΔA)	Positive	Increase wind

In general (22) contains four important terms

1) Term: $\frac{\Delta\gamma}{2 \cdot \gamma^2}$. The adiabatic constant decreases over

time due to the presence of larger pollutant molecules in the atmosphere. This effect tends to reduce wind speeds.

2) Term: $-\frac{(\gamma-1) \cdot T \cdot \Delta c_p}{\gamma \cdot 2 \cdot c_p}$. This term is associated with

changes in the specific heat capacity. A decrease in the specific heat capacity over time leads to a positive contribution of this term, which, together with the first term, results in a slower decrease in wind speed. If the second term is absent, the first term alone would lead to a faster decrease in wind speed.

3) Term: $-\frac{(\gamma-1)}{\gamma \cdot T} \cdot \left(\frac{\Delta Q}{m \cdot c} - \frac{Q \cdot \Delta m}{m^2 \cdot c} \right)$. This term represents the

thermal driving caused by excess heat and mass variations. Its value may be positive or negative depending on the magnitudes of ΔQ and Δm .

4) Term: $\frac{(\gamma-1) \cdot \Delta A}{\gamma \cdot T \cdot K}$. Wind speed variation depends on the

balance between thermodynamic changes ($\Delta\gamma, \Delta c_p$), thermal forcing ($\Delta Q, \Delta m$), and radiative effects (ΔA). Increased albedo from sulfate aerosols can enhance wind speed, while the first three terms cause thermodynamic damping. Wind increases or decreases depending on which effect dominates. Atmospheric regimes are summarized in Table 8.

To determine whether winds are damping or accelerating, a special ratio, called the feedback ratio (Φ), is defined.

$$\Phi = \frac{\text{Albedo term}}{\text{Therm-ic terms}} = \frac{\frac{\gamma-1}{\gamma T} \cdot \frac{\Delta A}{K}}{\left[\frac{\Delta \gamma}{2 \cdot \gamma^2} - \frac{(\gamma-1) \cdot T \cdot \Delta c_p}{\gamma \cdot 2 \cdot c_p} - \frac{(\gamma-1)}{\gamma \cdot T} \cdot \left(\frac{\Delta Q}{m \cdot c} - \frac{Q \cdot \Delta m}{m^2 \cdot c} \right) \right]} \quad (43)$$

If $\Phi < 1$, then wind decreases (polluted dominated regime).
If $\Phi > 1$, then wind increases (albedo dominated regime).
If $\Phi \approx 1$, then we have bistability or tipping points.

TABLE 8 IMPACT OF DIFFERENT ATMOSPHERIC REGIMES ON WIND VIA ALBEDO AND THERMODYNAMIC EFFECTS

Regime	Dominant Term	Net Effect on Wind
Clean atmosphere	Albedo term small	Slight decrease or stable
Marine aerosols	Albedo term moderate	Near-zero (stabilizing feedback)
Black carbon / PM _{2.5}	Thermodynamic terms dominate	Strong decrease (damping)
Hypothetical pure-albedo	Albedo term dominates	Wind increase (rare)

The regime of Pollution dominated or albedo dominated is presented in Table 9.

TABLE 9 SUMMARY OF POLLUTANT TYPES AND THEIR CORRESPONDING THERMODYNAMIC CHARACTERISTICS

Pollutant	γ	Type	Regime
Clean Air (N ₂ /O ₂)	1.40	Background	Clean
CO ₂	1.30	GHG	Pollution-Dominated (if dominant)
CH ₄	1.32	GHG	Pollution-Dominated
SO ₂	1.29	Scattering aerosol	Albedo-Dominated (if dominant)
Black Carbon	~1.06 (with PM)	Absorbing aerosol	Pollution-Dominated
PM _{2.5}	~1.06	Complex mix	Pollution-Dominated
Sea Salt	~1.33 (estimate)	Scattering	Albedo-Dominated

Then, (22) shows that wind speed is determined by a balance:

$$\frac{\Delta u}{u} = \text{Negative Therm-ic Terms} + \text{Positive Albedo Term}$$

Whether wind increases or decreases depends on which term dominates. The net effect on wind is presented in Table 10.

This relation shows two competing responses to pollution: thermodynamic damping, which reduces wind speed, and albedo forcing, which can enhance wind activity. The net effect depends on aerosol composition: clean or marine aerosols keep stable conditions, black

carbon and soot cause wind stilling, while volcanic or marine events may temporarily increase wind. Table 11 summarizes these effects through the feedback ratio Φ .

TABLE 10 SUMMARY OF ATMOSPHERIC REGIMES AND THEIR IMPACT ON WIND DYNAMICS

Regime	Dominant Term	Net Effect on Wind
Clean atmosphere	Albedo term small	Slight decrease or stable
Marine aerosols	Albedo term moderate	Near-zero (stabilizing feedback)
Black carbon/ PM _{2.5}	Thermodynamic terms dominate	Strong decrease (damping)
Hypothetical pure-albedo	Albedo term dominates	Wind increase (rare)

1) Albedo dominated regime $\Phi > 1$. This regime is described by more aerosols. For the albedo dominated regime is characteristic that this regime occurs when

$$\frac{(\gamma-1)}{\gamma T} \cdot \frac{\Delta A}{K} > |\text{Therm-ic Terms}| \quad (44)$$

Physical characteristics:

- Aerosols: mainly scattering (sulfates SO₄²⁻, sea salt, ammonium nitrate)
- Cloud effect: increased Cloud Condensation Nuclei (CCN) → smaller droplets → brighter clouds (Twomey effect)
- GHG levels: low-moderate (CO₂, CH₄ not dominant)
- Molecular effect: small $\Delta \gamma$ and Δc_p (minor change in composition)
- Result: wind slightly increases or remains stable.

2) Pollution dominated regime ($\Phi < 1$). This regime is described by more green house gases and absorbing aerosols. This regime occurs when:

$$\frac{(\gamma-1)}{\gamma T} \cdot \frac{\Delta A}{K} < |\text{Therm-ic Terms}| \quad (45)$$

Physical characteristics:

- Aerosol type: absorbing aerosols (black carbon, brown carbon, dust) + polyatomic gases (CO₂, CH₄, N₂O)
- Molecular effect: significant changes in $\Delta \gamma$ and Δc_p , altering air composition

Typical γ values:

Clean air: $\gamma \approx 1.40$

CO₂: $\gamma \approx 1.30$

CH₄: $\gamma \approx 1.32$

PM_{2.5}: $\gamma \approx 1.06$

Result: wind decreases due to thermodynamic damping.

TABLE 11 CLASSIFICATION OF ATMOSPHERIC FORCING REGIMES BASED ON AEROSOL AND GREENHOUSE GAS LOADING

Regime	Physical Meaning	Primary Driver	Aerosol Load	GHG Load
Albedo-Dominated ($\Phi > 1$)	Reflection effects dominate over thermodynamic effects	Scattering aerosols (sulfates, sea salt, clean clouds)	High	Low to Moderate
Pollution-Dominated ($\Phi < 1$)	Thermodynamic/molecular effects dominate	Absorbing aerosols + GHGs (black carbon, PM _{2.5} , CO ₂ , CH ₄)	High	High
Clean Regime ($\Phi \approx 1$)	No significant forcing	Natural background	Low	Low

Table 12 presents four atmospheric regimes defined by GHG and aerosol levels, showing their effects on radiative forcing (Φ) and wind patterns. GHGs enhance warming and circulation changes, while aerosols modify albedo and often reduce surface wind speed (“wind stalling”).

TABLE 12 CLIMATE INTERACTION MATRIX: GREENHOUSE GASES VS. AEROSOLS

	Low Aerosols	High Aerosols
Low GHGs	Clean Regime ($\Phi \approx 1$) • Natural winds • Small Δu	Albedo-Dominated ($\Phi > 1$) • Marine/volcanic • Wind stable or $\uparrow$
High GHGs	GHG-Only Warming • $\Delta T \uparrow$ • Complex wind	Pollution-Dominated ($\Phi < 1$) • BC + CO ₂ + CH ₄ • Wind stalling ($\Delta u/u < 0$)

CONCLUSIONS

This research established a combined model that connects thermodynamic properties of air with radiative feedback processes in order to explain how atmospheric pollution changes wind speed. The results show that pollution influences not only the chemical state of the atmosphere but also the basic physical principles that control air movement, convection, and energy transfer. One of the central findings concerns the thermodynamic modification of polluted air. In cleaner atmospheric conditions, the specific heat capacity of air is close to 1007 J/kg·K, while in strongly polluted environments it decreases to nearly 992 J/kg·K. At the same time, the adiabatic constant gamma decreases from 1.101 to 1.061. This variation corresponds to an increase in the effective molecular degrees of freedom from about 20 to nearly 33, indicating that pollution changes the way energy is distributed within atmospheric molecules.

These changes have a strong effect on the vertical thermal profile of the atmosphere. A lower value of the adiabatic constant causes weaker adiabatic cooling when air rises upward. As a result, atmospheric instability

becomes stronger, convection is modified, and vertical wind transport changes noticeably. This confirms that pollution directly affects the thermodynamic balance responsible for atmospheric circulation.

Another major result is the definition of different wind response regimes controlled by the feedback parameter Φ .

This ratio determines whether pollution produces weaker winds or supports stronger circulation. When $\Phi < 1$, the pollution-dominated regime is established. In this situation, thermodynamic damping becomes dominant and wind speed may decrease by up to 20 percent. This behavior is typical for black carbon, PM_{2.5} aerosols, and high greenhouse gas concentrations. When $\Phi > 1$, the atmosphere enters the albedo-dominated regime. Scattering aerosols such as sulfates and sea salt increase atmospheric reflectivity, which improves stability and can preserve or slightly increase wind speed. When $\Phi \approx 1$, the system reaches a critical transition region with bistable behavior. In this zone, small changes in aerosol composition may shift the atmosphere from one regime to another, creating tipping-point effects in wind dynamics.

An additional important result is the derived mathematical relation between relative wind speed variation ($\Delta u/u$) and changes in temperature (ΔT), specific heat capacity (Δc_p), adiabatic constant ($\Delta \gamma$), and albedo (ΔA). This equation shows the balance between thermodynamic suppression and radiative compensation. An increase in albedo ($\Delta A > 0$) can partly compensate for wind reduction by reflecting more incoming solar radiation. However, strongly absorbing aerosols such as black carbon dominate over this effect, leading to net wind stalling.

The practical applications of this work are broad. In climate modeling, it becomes necessary to include aerosol composition, especially the difference between scattering and absorbing particles, together with greenhouse gases for accurate prediction of atmospheric circulation. In air quality management, reducing black carbon and PM_{2.5} emissions can help prevent wind stalling and improve pollutant dispersion. For renewable energy planning, wind resource assessment should consider regional aerosol conditions, such as differences between marine and industrial zones. In urban planning, cities with high concentrations of absorbing aerosols may experience weaker ventilation, which can intensify heat island effects and increase pollution episodes.

The broader significance of the study is that pollution changes not only radiative forcing but also the fundamental thermodynamic properties of air itself. Ignoring these coupled effects may lead to serious errors in predicting wind patterns, storm behavior, and boundary-layer processes. Future climate studies should therefore include composition-dependent parameters of specific heat capacity and the adiabatic constant in order to describe the full anthropogenic impact on atmospheric circulation more accurately.

REFERENCES

- [1] Petrov, M., 2021. Adiabatic thermodynamic manner of the description of the carbon dioxide pollutant excess of Earth's atmosphere. In: *Proceedings of the V International Scientific Conference on Mathematical Modelling*, Borovets, Bulgaria, 8–11 December 2021. *Mathematical Modelling*, 5(3), 8–15.
- [2] U.S. Standard Atmosphere, 1976. Engineering ToolBox. Available at: https://www.engineeringtoolbox.com/standard-atmosphere-d_604.html
- [3] NASA Earth Observatory, 2023. World of Change: Global Temperatures. <https://earthobservatory.nasa.gov/world-of-change/global-temperatures>
- [4] Copernicus Climate Change Service, 2019. Last four years have been the warmest on record and CO₂ continues to rise. <https://climate.copernicus.eu>
- [5] Electrical and Mechanical Services Department (EMSD), 2023. *Energyland: Greenhouse Gases*. Government of the Hong Kong Special Administrative Region. Available at: <https://www.emsd.gov.hk/energyland>
- [6] Petrov, M., 2021. Major contribution of carbon dioxide excess in atmosphere to the greenhouse effect. *Oxidation Communications*, 44(4), 870–907.
- [7] Antweiler, W., 2015. *Fossil fuels and declining oxygen in our atmosphere*. Available at: <https://wernerantweiler.ca/blog.php?item=2015-10-15>
- [8] Vashishta, M., Sharma, P., 2014. Variation of specific heat ratio. *International Journal of Engineering and Advanced Technology*, 3(4), 213–217.
- [9] Seinfeld, J.H., Pandis, S.N., 2016. *Atmospheric Chemistry and Physics: From Air Pollution to Climate Change*, 3rd ed. Wiley, Hoboken, NJ.
- [10] Manatung, S.S., Latimer, D.C., 2019. Heat capacity ratios of real gases. *Journal of Chemical Education*, 96, 1694–1700. <https://doi.org/10.1021/acs.jchemed.9b00060>
- [11] Wejlal, A.K., 2025. Thermophysical properties of atmospheric gases. *South Eastern European Journal of Public Health*, 26(S2), pp. 3809–3817. <https://doi.org/10.70135/seejph.vi.5859>
- [12] Petrov, M., et al., 2025. Influence of greenhouse pollutants on adiabatic constant. In: *Modelling and Development of Intelligent Systems*. Springer.
- [13] White, F.M., 2011. *Fluid Mechanics*, 7th ed. McGraw-Hill.
- [14] Chen, R.H., 2017. *Foundations of Gas Dynamics*. Cambridge University Press.
- [15] Twomey, S., 1977. The influence of pollution on the shortwave albedo of clouds. *Journal of the Atmospheric Sciences*, 34, 1149–1152. [https://doi.org/10.1175/1520-0469\(1977\)034<1149:TIOPOT>2.0.CO;2](https://doi.org/10.1175/1520-0469(1977)034<1149:TIOPOT>2.0.CO;2)
- [16] Lohmann, U., Feichter, J., 2005. Global indirect aerosol effects: a review. *Atmospheric Chemistry and Physics*, 5, 715–737. <https://doi.org/10.5194/acp-5-715-2005>
- [17] Ritchie, H., Roser, M., 2021. *Deforestation and Forest Loss*. Our World in Data. Available at: <https://ourworldindata.org/deforestation>
- [18] Hansen, J., Nazarenko, L., 2004. Soot climate forcing via snow and ice albedos. *PNAS*, 101(2), 423–428. <https://doi.org/10.1073/pnas.2237157100>
- [19] Menon, S., et al., 2010. Radiative forcing and temperature response to changes in urban albedos. *Environmental Research Letters*, 5(1). <https://doi.org/10.1088/1748-9326/5/1/014005>
- [20] Cugliandolo, L.F., 2011. Effective temperature of the Earth. *Journal of Physics A*, 44, 483001. <https://doi.org/10.1088/1751-8113/44/48/483001>
- [21] Latham, J., Smith, M.H., 1990. Effect on global warming of wind-dependent aerosol generation. *Nature*, 347, 372–373. <https://doi.org/10.1038/347372a0>
- [22] Ramanathan, V., Carmichael, G., 2008. Global and regional climate changes due to black carbon. *Nature Geoscience*, 1, 221–227. <https://doi.org/10.1038/ngeo156>
- [23] Lide, D.R. (Ed.), 1996. *CRC Handbook of Chemistry and Physics*, 77th ed. CRC Press, Boca Raton.
- [24] Kelly, M., Monroe, R., 2018. *Earth's oceans have absorbed 60 percent more heat per year than previously thought*. Princeton University. Available at: <https://www.princeton.edu/news/2018/10/31>
- [25] Berlinger, J., Smith-Spark, L., 2018. *World's oceans have absorbed 60 percent more heat than previously thought*. CNN. Available at: <https://edition.cnn.com/2018/10/31/world/ocean-warming-study>
- [26] McCarthy, J., 2018. *Oceans have absorbed 60 percent more heat than previously thought*. Global Citizen. Available at: <https://www.globalcitizen.org>
- [27] Shutler, J., Watson, A., 2020. *The oceans are absorbing more carbon than previously thought*. Carbon Brief. Available at: <https://www.carbonbrief.org>
- [28] Oceanographic Magazine, 2021. *Rate of CO₂ absorption by ocean impacted by human-caused atmospheric changes*. Available at: <https://www.oceanographicmagazine.com>
- [29] Picone, J.M., Hedin, A.E., Drob, D.P., Aikin, A.C., 2002. NRLMSISE-00 empirical model of the atmosphere. *Journal of Geophysical Research: Space Physics*, 107(A12), 1468. <https://doi.org/10.1029/2002JA009430>
- [30] Chemke, R., Kaspi, Y., Halevy, I., 2016. The thermodynamic effect of atmospheric mass on early Earth's temperature. *Geophysical Research Letters*, 43, 11414–11422. <https://doi.org/10.1002/2016GL071279>
- [31] Best, C., 2016. *The atmosphere is getting heavier*. Available at: <https://clivebest.com/blog/?p=7704>
- [32] Raju, D., Ramdin, M., Vlugt, T.J.H., 2024. Thermophysical properties of CO₂ with impurities. *Journal of Chemical & Engineering Data*, 69(8), 2735–2755. <https://doi.org/10.1021/acs.jced.4c00164>
- [33] Ning, F.L., et al., 2015. Heat capacity of CH₄-CO₂ mixtures. *Physical Chemistry Chemical Physics*, 17, 2869–2883. <https://doi.org/10.1039/C4CP04725A>
- [34] Colman, R., 2021. Water vapor and lapse rate feedbacks. *Reviews of Modern Physics*, 93, 045002. <https://doi.org/10.1103/RevModPhys.93.045002>
- [35] Manabe, S., 2019. Role of greenhouse gases in climate change. *Climate Dynamics*, 53, 113–129. <https://doi.org/10.1007/s00382-018-4137-6>
- [36] Henry, M., Merlis, T.M., 2020. Forcing dependence of atmospheric lapse rate changes. *Geophysical Research Letters*, 47, e2020GL087929. <https://doi.org/10.1029/2020GL087929>
- [37] Brogli, R., et al., 2021. Lapse rate effects on future summer warming. *Weather and Climate Dynamics*, 2, 1093–1110. <https://doi.org/10.5194/wcd-2-1093-2021>
- [38] Wong, G.S.K., Embleton, T.F.W., 1984. Variation of specific heats in humid air. *Journal of the Acoustical Society of America*, 76, 555–559. <https://doi.org/10.1121/1.391002>
- [39] Liepmann, H.W., Roshko, A., 2001. *Elements of Gasdynamics*. Dover.
- [40] Liou, K.N., 2002. *An Introduction to Atmospheric Radiation*, 2nd ed. Academic Press. <https://doi.org/10.1016/B978-012451451-5/50001-8>
- [41] Ramanathan, V., Crutzen, P.J., Kiehl, J.T., Rosenfeld, D., 2001. Aerosols, climate, and the hydrological cycle. *Science*, 294(5549), 2119–2124. <https://doi.org/10.1126/science.1064034>
- [42] Merenda, B., et al., 2024. PM variability and meteorology. *Scientific Reports*, 14, 19461. <https://doi.org/10.1038/s41598-024-19461>
- [43] Twomey, S., 1974. Pollution and the planetary albedo. *Atmospheric Environment*, 8, 1251–1256. [https://doi.org/10.1016/0004-6981\(74\)90004-3](https://doi.org/10.1016/0004-6981(74)90004-3)
- [44] Andreae, M.O., Rosenfeld, D., 2008. Aerosol–cloud–precipitation interactions. *Earth-Science Reviews*, 89, 13–41. <https://doi.org/10.1016/j.earscirev.2008.03.001>
- [45] Bond, T.C., et al., 2013. Bounding the role of black carbon in the climate system. *Journal of Geophysical Research*, 118, 5380–5552. <https://doi.org/10.1002/jgrd.50171>
- [46] Wild, M., 2009. Global dimming and brightening. *Journal of Geophysical Research*, 114. <https://doi.org/10.1029/2008JD011470>

- [47] Oke, T.R., 1987. *Boundary Layer Climates*, 2nd ed. Routledge.
- [48] Petrov, M., 2022. Relational empirical study of outgoing longwave radiation–albedo–temperature of the atmosphere–Earth system under the influence of carbon dioxide pollutants. *Oxidation Communications*, 45(2), 350–382.
- [49] IPCC, 2021. *Climate Change 2021: The Physical Science Basis*. Cambridge University Press. <https://www.ipcc.ch/report/ar6/wg1>
- [50] Wallace, J.M., Hobbs, P.V., 2006. *Atmospheric Science: An Introductory Survey*, 2nd ed. Academic Press.
- [51] Holton, J.R., Hakim, G.J., 2013. *An Introduction to Dynamic Meteorology*, 5th ed. Academic Press.
- [52] Landau, L.D., Lifshitz, E.M., 1980. *Statistical Physics. Part 1*, 3rd ed. Pergamon Press, Oxford. <https://doi.org/10.1016/C2009-0-07734-5>
- [53] Lemmon, E.W., Jacobsen, R.T., Penoncello, S.G., Friend, D.G., 2000. Thermodynamic properties of air and mixtures of nitrogen, argon, and oxygen from 60 to 2000 K. *Journal of Physical and Chemical Reference Data*, 29(3), 331–385. <https://doi.org/10.1063/1.1285884>
- [54] Trenberth, K.E., Smith, L., 2004. The mass of the atmosphere: A constraint on global analyses. *Journal of Climate*, 17, 864–875. [https://doi.org/10.1175/1520-0442\(2004\)017<0864:TMOATA>2.0.CO;2](https://doi.org/10.1175/1520-0442(2004)017<0864:TMOATA>2.0.CO;2)
- [55] Ball, P., 2003. Global greenhouse effects air pressure. *Nature*, 422, 245. <https://doi.org/10.1038/422245a>
- [56] Almousa, N., et al., 2021. Paraffin wax composites for thermal energy storage. *Crystals*, 11, 951. <https://doi.org/10.3390/cryst11080951>
- [57] Mayer, H., 2000. Air pollution in cities. *Solar Energy*, 69(6), 427–436. [https://doi.org/10.1016/S0038-092X\(00\)00004-1](https://doi.org/10.1016/S0038-092X(00)00004-1)
- [58] Zha, J., et al., 2021. Aerosol forcing and wind stilling. *Environmental Research Letters*, 16, 064002. <https://doi.org/10.1088/1748-9326/ac02c8>
- [59] Mason, E.A., Saxena, S.C., 1958. Transport properties of gases. *Physics of Fluids*, 1(5), 361–369. <https://doi.org/10.1063/1.1724352>
- [60] Pruppacher, H.R., Klett, J.D., 2010. *Microphysics of Clouds and Precipitation*, 2nd ed. Springer.
- [61] Berberan-Santos, M.N., et al., 2005. On the barometric formula. *American Journal of Physics*, 73, 914–923. <https://doi.org/10.1119/1.1900108>
- [62] Lemmon, E.W., Jacobsen, R.T., 2004. Transport properties of air. *Journal of Physical and Chemical Reference Data*, 33, 195–235. <https://doi.org/10.1063/1.1645272>
- [63] Myhre, G., et al., 2013. Anthropogenic and natural radiative forcing. In: *Climate Change 2013: The Physical Science Basis*. Cambridge University Press.
- [64] Bohren, C.F., Albrecht, B.A., 2000. *Atmospheric Thermodynamics*. Oxford University Press.
- [65] Stull, R.B., 1988. *Boundary Layer Meteorology*. Springer.
- [66] Petrov, M., et al., 2024. *Thermodynamic empirism for atmospheric pollutants*. *Environment. Technology. Resources*, 1, pp. 300–305.
- [67] Fuchs, R., Glasser, L., 2022. Rüchardt experiment. Springer.
- [68] Shaw, T.A., 2025. Moist adiabatic scaling. *Geophysical Research Letters*, 52(7).
- [69] Yang, Q., et al., 2017. *PM_{2.5} and meteorological factors*. arXiv preprint. Available at: <https://arxiv.org>
- [70] Ames, F.E., Tang, C.C., 2021. *Compressible Flow*. CRC Press.
- [71] Kundu, P.K., et al., 2015. *Fluid Mechanics*, 6th ed. Academic Press.
- [72] Su, T., et al., 2020. Aerosol-boundary layer feedback. *Journal of Geophysical Research: Atmospheres*, 125. <https://doi.org/10.1029/2019JD031975>
- [73] Zhang, Y., et al., 2020. Dome effect of black carbon. *Atmospheric Research*, 239, 104921. <https://doi.org/10.1016/j.atmosres.2019.104921>
- [74] Naydenova, S., et al., 2022. PAHs in PM_{2.5} and PM₁₀. *Journal of Environmental Science and Health A*, 57, 1–12. <https://doi.org/10.1080/10934529.2022.2036789>
- [75] Nikolaeva, Z., et al., 2017. *Atmospheric transparency and PM₁₀*. *International Journal of Scientific Engineering and Applied Science*, 3(5), pp. 109–114.
- [76] Dimitrov, A., Naydenova, S., 2025. Black carbon in PM_{2.5}. *Atmosphere*, 16(2), 412. <https://doi.org/10.3390/atmos16020412>
- [77] Gui, K., et al., 2021. Aerosol–boundary layer feedback. *Environment International*, 157, 106861. <https://doi.org/10.1016/j.envint.2021.106861>
- [78] Ren, Y., et al., 2021. Aerosol-boundary layer feedback. *Atmospheric Chemistry and Physics*, 21, 9033–9047. <https://doi.org/10.5194/acp-21-9033-2021>
- [79] Dimitrov, A., Naydenova, S., 2023. Thermodynamic damping of wind velocity. *Journal of Atmospheric and Solar-Terrestrial Physics*, 248, 106004. <https://doi.org/10.1016/j.jastp.2023.106004>
- [80] Naydenova, S., et al., 2022. *Atmospheric PM levels*. *Journal of Environmental Science and Health, Part A*, 57, pp. 1–12. <https://doi.org/10.1080/10934529.2022.2036789>
- [81] Dimitrov, A., 2021. Adiabatic processes in polluted atmospheres. *Bulgarian Chemical Communications*, 53(A), 112–118.
- [82] Dimitrov, A., Naydenova, S., 2025. Black carbon and meteorology. In: *Proceedings of the VII ICABLS*, pp. 1023–1034.
- [83] Hartmann, D.L., 2016. *Global Physical Climatology*, 2nd ed. Elsevier. <https://doi.org/10.1016/C2012-0-04052-0>
- [84] Hansen, J., Sato, M., Ruedy, R., 1997. Radiative forcing and climate response. *Journal of Geophysical Research*, 102(D6), 6831–6864. <https://doi.org/10.1029/96JD03436>

Integrated Risk Assessment Model for Cyber Threats to Critical Infrastructure

Irena Petrova

*Dept of Technology, Organization
and Management of Transport*

Todor Kableshkov University of Transport, Sofia, Bulgaria
ipetrova@vtu.bg

ORCID: [0009-0001-6321-7210](https://orcid.org/0009-0001-6321-7210)

Kostadin Trifonov

*Dept of Technology, Organization
and Management of Transport*

Todor Kableshkov University of Transport, Sofia, Bulgaria
ktrifonov@vtu.bg

ORCID: [0000-0002-9130-483X](https://orcid.org/0000-0002-9130-483X)

Abstract—Critical infrastructure has become increasingly vulnerable to complex cyber threats characteristic of the contemporary hybrid security environment. The convergence of digital attacks, information operations, and potential physical disruptions necessitates integrated risk assessment approaches that capture both technological and operational dimensions of infrastructure systems. This study presents an integrated risk assessment model for cyber threats targeting critical infrastructure, combining artificial intelligence (AI) techniques with expert transport-system analysis, with a specific focus on railway infrastructure as a key component of national security. The proposed model comprises: (1) an AI-based anomaly detection module; (2) probabilistic hybrid-threat modeling; and (3) a transport-logistics resilience assessment. Simulation results demonstrate higher accuracy in risk prediction, earlier detection of critical deviations, and more effective planning of protective measures. The model supports identifying the most vulnerable infrastructure elements and developing adaptive response strategies.

Keywords—critical infrastructure, cybersecurity, hybrid threats, railway systems.

I. INTRODUCTION

Railway infrastructure has maintained strategic significance in national security for over a century. Railways remain essential for the movement of people, goods, and military assets. The increasing deployment of digital control systems has further elevated the sector's importance while expanding its vulnerability to hostile interference [1], [2].

Critical infrastructure (CI) represents the backbone of national security, economic security, and social functioning [3]. Increasing digitalization, automation, and interconnectivity have expanded the attack surface of CI systems [4]. Modern cyberattacks take the form of hybrid operations that combine cyber intrusions, misinformation, and physical disruptions, simultaneously leveraging

vulnerabilities across technological, operational, and organizational layers. The global railway cybersecurity market reflects this urgency: valued at USD 8.0 billion in 2024, it is projected to reach USD 16.0 billion by 2033, growing at a CAGR of 7.98% [5], while concurrent estimates indicate a compound annual growth rate of 8.62% through 2032 [6].

Railway systems are particularly exposed due to their reliance on signaling and interlocking systems, communication networks, SCADA-based energy subsystems, and tightly coupled operational processes [7]. Even short-term disruptions might propagate rapidly, causing cascading delays, safety risks, and operational degradation. The consequences go beyond the railway sector itself, carrying deep implications for national security and public welfare.

Conventional risk assessment frameworks were built around single-vector threats; they systematically underestimate scenarios in which cyber intrusion, physical sabotage, and disinformation operate in sequence [8], [9], [10]. Measuring and quantifying cybersecurity performance is itself a major challenge: as Brothby and Hinson [11] demonstrate, effective cybersecurity metrics must be both SMART and PRAGMATIC — specific, measurable, actionable, and time-dependent — to support meaningful decision-making. Machine learning methods can detect deviations in control-system behaviour within seconds — a response window that manual monitoring cannot match [12]. Continuous monitoring alone is insufficient: without automated response logic, anomaly detection flags events too late for human operators to intervene before cascading failures propagate [13]. Purpose-built cybersecurity risk assessment software further supports this by automating risk register maintenance, quantifying threat impact, and guaranteeing alignment with frameworks such as NIST CSF and ISO 27001 [14].

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.134>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

This study introduces an integrated risk assessment model that incorporates AI-based anomaly detection, probabilistic hybrid threat modeling, and transport logistics resilience analysis. The model facilitates vulnerability identification, prediction of cascading failures, and improved operational continuity in the context of hybrid threats.

II. LITERATURE REVIEW ON THE RESEARCH TOPIC

Research on cyber-physical security has expanded substantially over the past decade, motivated by the increasing complexity, interconnectivity, and digitalization of critical infrastructure systems. Foundational surveys such as Humayed et al. [3] and Flammini [15] emphasize that modern cyber-physical systems (CPS) exhibit tightly coupled operational, communication, and control layers, in which disruptions in one domain rapidly propagate to others. For sectors such as rail and energy — where a 15-minute outage can trigger national-level consequences — this interdependence makes CPS security a first-order engineering problem, not a compliance exercise.

The shift from isolated intrusions to coordinated hybrid operations is now well-documented. Early analyses of industrial cyber incidents — most notably the Stuxnet case examined by Karnouskos [8] — demonstrated that cyberattacks can directly cause physical consequences. More recent studies, such as those by Rass et al. [16] and Hahn et al. [17], show that adversaries increasingly combine cyber intrusions, physical sabotage, and information manipulation to amplify their impact. Hybrid threat modeling structures, therefore, incorporate probabilistic reasoning, attack graph analysis, and scenario-driven simulation to model nonlinear escalation patterns [9], [18]. The inherent nature of these threats is not confined to railways but extends across all digitized transport domains. In the maritime sector, GPS and AIS spoofing attacks have escalated sharply, with over 1,000 vessels per day reportedly affected by signal interference in the Persian Gulf and Strait of Hormuz [19]. At the same time, government-backed actors have targeted port logistics, classification societies, and ship communications [20]. In aviation, a pro-Russian hacktivist group, Killnet, executed a sustained DDoS offensive against EUROCONTROL in April 2023, disrupting the European air traffic management agency's communication systems and forcing airlines onto backup procedures [21]; earlier, researchers demonstrated that legacy ACARS and ADS-B protocols could be exploited to manipulate aircraft navigation data with few barriers [22]. In the space domain, the most consequential documented attack occurred on 24 February 2022, one hour before Russia invaded Ukraine, when Russian GRU actors deployed AcidRain wiper malware against Viasat's KA-SAT satellite network, turning off tens of thousands of modems across Ukraine and Europe, causing the malfunction of 5,800 wind turbines in Germany, and disrupting Ukrainian military command and control [23]. Finally, penetration testing of public EV charging infrastructure has revealed analogous vulnerability surfaces — availability disruption, data manipulation, and authentication bypass [13], [24] — confirming that cyber-physical vulnerabilities follow

consistent cross-sector patterns across all interconnected transport and energy systems.

Within the transport domain, railway systems have become a critical focus area due to their reliance on signaling, interlocking, communication networks, and SCADA-based energy subsystems. Yilmaz et al. [7] and Ghafouri et al. [25] document the growing vulnerability of railway signaling systems to cyber intrusions, noting that even short-duration disruptions might trigger cascading operational failures. Maranco et al. [26] further demonstrate that intelligent transportation systems are increasingly exposed to communication interference, GNSS spoofing, and coordinated cyber-physical attacks. These data emphasize the need for consolidated security systems that account for both cyber and operational dimensions of railway infrastructure. Ibadah, Benavente-Peces, and Pahl [27] further extend this analysis to on-board and trackside sensor networks, cataloging protocol-level vulnerabilities in MVB and CAN communications and proposing a multi-tiered security architecture for railway cyber-physical systems. The transition to the Future Railway Mobile Communication System (FRMCS) introduces additional identity management and access-control requirements that further expand the attack surface of digitalized railway networks, necessitating service-oriented security architectures aligned with the evolving FRMCS specification [28].

Artificial intelligence has become a central element of modern intrusion detection and cyber-physical monitoring. Machine learning-based anomaly detection techniques — including SVMs, Recurrent neural networks, autoencoders, and unsupervised outlier detection — have been shown to outperform traditional expert systems in detecting subtle irregularities in CPS behavior [29]. Wang et al. [30] and Taaama [12] further demonstrate that deep learning models can detect temporal and organizational patterns in industrial control data, enabling earlier detection of malicious activity. These AI-powered approaches are increasingly being applied in transport management systems as part of broader digitalization efforts [31]. Systematic mapping studies further confirm the growing deployment of AI across offensive and defensive cybersecurity scenarios — including detection, automated response, and threat intelligence applications [32].

Resilience research complements cybersecurity studies by examining how infrastructure systems absorb, adapt to, and recover from disruptions. Flammini [15] and Z. Wang, X. Liu [33] highlight that resilience metrics — such as delay propagation, redundancy, safety margins, and recovery time — are key for assessing the operational consequences of cyber incidents. Dimitrov, Zlateva, and Velev [34] propose a GIS-based hazard classification framework for transport infrastructure, showing how real-time information can support resilience-oriented decision-making. These procedures address the need for resilience assessment in cyber-physical railway environments.

Quantification remains the weakest link in most frameworks. Brotby and Hinson [11] are direct on this: metrics that cannot be expressed as specific, measurable, time-bound values offer decision-makers no actionable

guidance. This perspective is consistent with the growing trend toward integrated, multi-criteria risk evaluation models that combine anomaly detection, probabilistic threat modeling, and toughness evaluation. Ali et al. [35] further confirm the effectiveness of combined ML and DL frameworks on critical infrastructure datasets, achieving LSTM accuracy of 99% — results that support the strategic value of AI-powered approaches adopted in the present study.

Market patterns reinforce the investment case for advanced rail cybersecurity. The global rail cybersecurity market, valued at US\$ 7.42 billion in 2023, is projected to grow at a CAGR of 8.62% through 2032 [6], driven by the digitalization of signaling, IoT integration, and rising regulatory pressure. Infrastructure accounted for 62% of revenues in 2024, underscoring the priority of protecting rail and control systems [5]. This trajectory confirms that IRAM's quantitative risk assessment capabilities are not merely technically justified but also economically necessary for operators seeking to comply with evolving national and EU cybersecurity obligations.

In the Bulgarian railway sector, the regulatory framework functions at two interrelated levels. At the national level, the Cybersecurity Act (promulgated as SG No. 94/2018; amended as SG No. 17/2026) designates railway infrastructure managers and undertakings as operators of vital services and requires them to implement risk management measures within the national cybersecurity management system. At the sectoral level, the Railway Transport Act and Ordinance No. 58 on Technical Operation, Train Traffic, and Signaling establish safety requirements that are directly linked to cybersecurity obligations for signaling, communication, and operational control systems.

The newly adopted Public Transport Act (in force since April 2026) [36] further expands the regulatory system by introducing an integrated national mobility framework, which includes a unified electronic ticket for rail, metro, and bus transport. Although intended to enhance interoperability and passenger convenience, this unified ticketing infrastructure also constitutes a potential cyberattack surface, thereby increasing the necessity for robust protection of payment, identity, and validation systems.

The transposition of Directive (EU) 2022/2555 (NIS2) will introduce stricter governance requirements, supply chain security, vulnerability disclosure, and stepwise incident reporting—24-hour early notification, 72-hour detailed reporting, and a final report within one month [37]. GDPR applies to all systems that process passenger data, including ticketing platforms, video surveillance systems, and passenger information systems. This multilayered regulatory environment requires railway operators to maintain quantifiable, auditable, and methodologically consistent risk assessment processes. The proposed Integrated Risk Assessment Model (IRAM) meets these requirements through the composite S score and the Resilience Index, providing measurable and time-stamped results aligned with the national framework [38] and EU

obligations [37], an approach further supported by the sector-specific cybersecurity analysis in source [27].

Taken together, the reviewed studies point toward the same gap: no existing framework simultaneously addresses anomaly detection, hybrid-threat scoring, and resilience quantification for railway systems. This paper targets that specific combination.

Contemporary studies on cyber-physical security of railway infrastructure converge around three major thematic domains: (1) AI-based detection, encompassing machine-learning techniques and anomaly-detection systems; (2) hybrid-threat modeling, covering cyber-physical attacks, probability analysis, and scenario-driven modeling; and (3) resilience and recovery, focusing on infrastructure robustness, operational impact, and recovery strategies. These domains converge into the central research focus of the present study: integrated cyber-physical risk assessment for railway infrastructure.

III. MATERIALS AND METHODS

The model is built around three coupled components: AI-based anomaly detection, probabilistic hybrid-threat modeling, and transport-logistics resilience assessment. The three components are deliberately sequenced: detection identifies the attack, threat modeling estimates its likely trajectory, and resilience assessment quantifies the operational damage if containment fails.

A. AI-Based Anomaly Detection Module

The anomaly detection module identifies variations from normal operational behavior in real time across signaling, communication, and control systems. It incorporates supervised and unsupervised machine learning techniques to detect known and unknown attack patterns [30]. The system integrates: Support Vector Machines (SVM); Isolation Forest for unsupervised outlier detection [29]; LSTM recurrent neural networks for temporal pattern modeling; and Autoencoders for reconstruction-based anomaly scoring [39]. Validation of these detection methods in industrial control system testbed environments further confirms their applicability to real-world railway cyber-physical systems [40]. The simulation dataset is composed of synthetic attack sequences generated in accordance with MITRE ATT'CK for ICS (tactics T0800–T0882), calibrated against documented incident parameters from the ENISA Railway Cybersecurity report [1] and the UIC Digital Transformation guidelines [2].

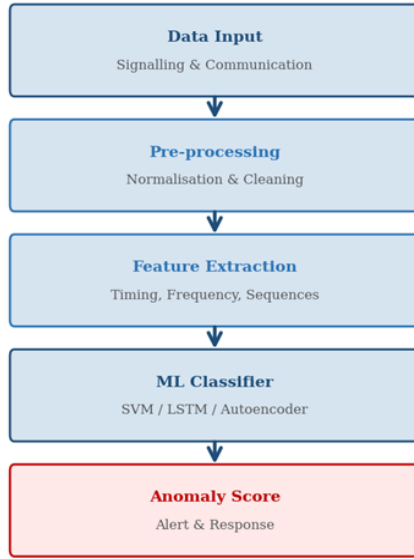


Fig. 1. AI-based anomaly detection module pipeline — from data acquisition to anomaly scoring.

B. Probabilistic Hybrid-Threat Modeling

Hybrid threats combine cyber intrusions, physical disruptions, and information manipulation to produce non-linear, emergent risks [41]. The Hybrid Risk Score (HRS) combines the threat probability $P(T)$, the estimated impact $I(T)$, and a cross-domain amplification factor $\Phi(C, Ph, I) = 3.39$, calibrated from historical incident data [16]. The module employs Bayesian networks, Markov chains, attack trees [18], and Monte Carlo simulation across large scenario sets [42].

C. Transport-Logistics Resilience Assessment

This component evaluates the operational impact of cyber disruptions on railway performance [25], [43]. The Resilience Index (RI) measures the ability to maintain operational continuity under attack. Delay propagation is modeled as a network diffusion process with coefficient $\lambda = 0.68$ for interlocking-dense segments [26]. The framework quantifies capacity utilization, delay propagation, redundancy, safety margins, and recovery time [33].

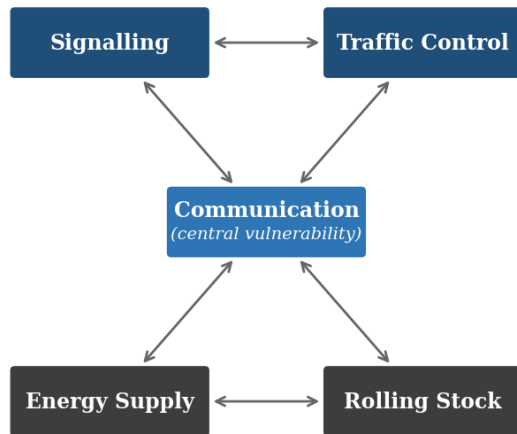


Fig. 2. Structural representation of subsystem interdependencies within railway infrastructure.

IV. RESULTS AND DISCUSSION

A. AI-Based Detection Performance

The results presented in this section were obtained from an AI-driven simulation using input parameters derived from MITRE ATT'CK for ICS synthetic attack sequences and domain-specific railway infrastructure parameters sourced from the ENISA Railway Cybersecurity report [1] and UIC guidelines [2]. The model has not been tested in a live operational environment; all quantitative outputs represent simulation results generated by calibrating the IRAM against documented incidents and validated benchmarks from prior research. This approach follows established practice in cyber-physical risk modeling, where direct real-world experimentation on safety-critical infrastructure is neither feasible nor permissible [40]. The AI-based anomaly detection module, fed with historical signaling anomaly profiles and synthetic attack sequences derived from the literature, produced the following simulation outputs: 94.2% overall detection accuracy, 87% reduction in false negatives versus rule-based baseline systems [39], and 0.8–1.2 s earlier detection of signaling anomalies compared to threshold-based methods. These figures are consistent with Ali et al. [35], who demonstrated LSTM and SVM accuracies of 99% and 98%, respectively, on cybersecurity benchmark datasets, confirming that AI-based detection is operationally superior to rule-based approaches. Testbed-based evaluations under controlled ICS conditions further corroborate these simulation results [40].

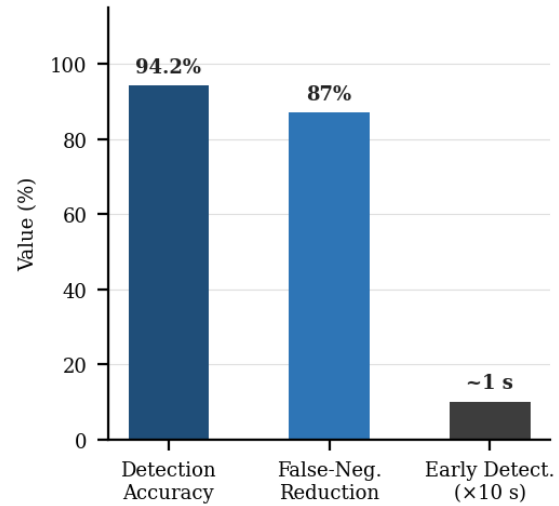


Fig. 3. Performance metrics — detection accuracy, false negative reduction, and detection speed.

Within the simulation framework, LSTM temporal networks and autoencoders exhibited superior performance in detecting timing manipulation, spoofed commands, and unauthorized configuration changes, which are attack patterns derived from historical incident records used as model input. These capabilities are particularly relevant to intelligent rail management systems [44], where the

complexity of automated control introduces additional surfaces of vulnerability that necessitate continuous AI-driven monitoring. These figures reflect simulation outputs calibrated against documented incidents, not field measurements. Real deployments will differ — legacy signaling architectures and attacker capability vary considerably across European rail operators.

B. Hybrid-Threat Scenario Analysis

Monte Carlo-based scenario analysis was conducted using input parameters calibrated from documented hybrid-threat incidents in the railway sector and adjacent critical infrastructure domains. Three representative scenarios were simulated across 10,000 iterations to produce statistically robust risk estimates: (1) Isolated cyber intrusion: HRS = 2.3 (moderate risk); (2) Combined cyber-physical attack: HRS = 5.1 (high risk); (3) Full hybrid operation: HRS = 7.8 (critical risk). The simulation results indicate that a full-hybrid operation generates systemic risk that is 3.3 times greater than that of an isolated cyber intrusion. The non-linear amplification factor $\Phi = 3.39$ — derived from calibration against historical multi-vector attack data — confirms that adversaries consistently leverage combined approaches, consistent with hybrid threat models documented in the scientific literature [16]. These are model outputs. An operator deploying IRAM in a specific network would need to recalibrate Φ against their own incident history and threat intelligence feeds.

A documented real-world case that directly validates the hybrid-threat scenario analysis above is the January 2022 cyberattack on Belarusian Railways (Belarusian Railways / Беларуская чыгунка), carried out by the hacktivist group Belarusian Cyber-Partisans [45]. The group encrypted the servers, databases, and workstations of the state-owned rail operator, disrupting ticket sales and online services, while explicitly refraining from targeting safety-critical automation and signaling systems to avoid endangering passengers [46]. The stated objective was to obstruct the movement of Russian troops through Belarusian territory in the context of the imminent invasion of Ukraine — making this the first publicly documented instance of politically motivated ransomware used to interfere with military logistics via civilian railway infrastructure [45], [46]. The attack confirms that railway IT systems constitute a viable entry point for hybrid operations that combine cyber disruption with geopolitical objectives, precisely the scenario captured by the combined cyber-physical attack (HRS = 5.1) in the present model. Notably, the attackers' deliberate exclusion of safety systems underscores the asymmetric nature of railway cyber threats: adversaries can calibrate their impact to

avoid triggering safety responses, thereby prolonging operational disruption while remaining below the threshold for a declared safety incident.

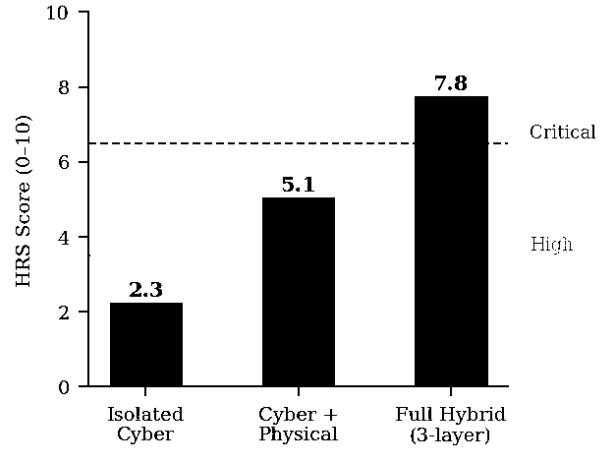


Fig. 4. Comparison of hybrid-threat risk scores across three attack scenarios.

C. Cascading Failure Propagation

Cascading failure propagation was modeled using a network diffusion approach, with input parameters derived from documented railway disruption timelines and operational performance data from the scientific literature. The simulation produced the following projected timeline for a successful cyber intrusion: initial signaling errors propagate to routing conflicts within 5–12 s; delay cascades emerge within 40–90 s; network-wide collapse occurs within 3–7 min in critical scenarios. The propagation coefficient $\lambda = 0.68$ — calibrated against historical cascade data — indicates that each affected node transmits 68% of accumulated delay to adjacent nodes within one time step. Based on these simulation parameters, the model projects that human operators cannot reliably respond within the critical 15s window following the onset of the initial anomaly, reinforcing the operational case for automated AI-driven detection. Field validation against real disruption logs would be required before these timelines could be used for staffing or response planning.

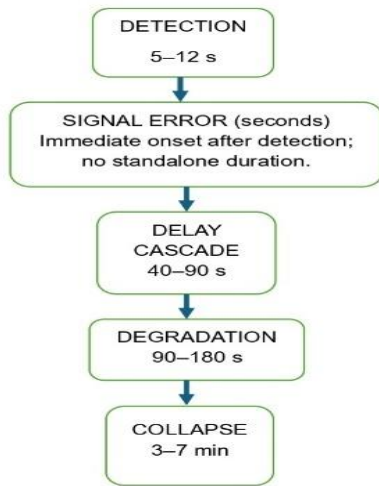


Fig. 5. Timeline of cascading failure propagation from initial intrusion to network collapse.

The simulated temporal propagation of cascading failures — as modeled by the IRAM using historical input data — begins with the onset of AI-detected anomalies and culminates in projected full operational collapse under an unmitigated hybrid-attack scenario.

D. Resilience Assessment

The Resilience Index (RI) was computed for three simulated attack conditions using input parameters drawn from historical incident reports and validated infrastructure performance benchmarks. Simulation results project the following degradation profile under attack: RI drops from 1.0 (baseline) to 0.71–0.79; capacity utilization decreases by 18–32%; delay propagation increases 45–70%; safety margins are reduced by up to 22%; and recovery time increases from 4 min to 11–17 min — a projected increase of up to 260%. These simulated degradation patterns closely mirror the disaster-impact phases defined in the infrastructure monitoring framework of Dimitrov, Zlateva, and Velez [34], providing cross-validation of the simulation outputs against independently published infrastructure resilience models. The RI values reported here are model projections based on simulated inputs; actual resilience outcomes in a deployed railway system would depend on specific network topology, redundancy configurations, and operator response capabilities.

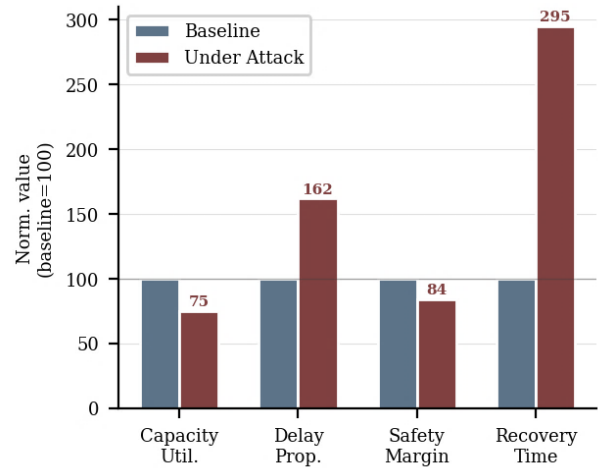


Fig. 6. Resilience indicator degradation — baseline vs. hybrid-attack conditions.

E. Comparative Analysis

Table I compares the proposed IRAM with representative prior frameworks identified in the literature review. The evaluation considers four dimensions pertinent to railway cyber-physical security. The performance indicators reported for the proposed model (94.2% detection accuracy, $\Phi=3.39$, RI range) are simulation outputs generated by the AI-driven model using historical data as input, rather than results from a deployed system evaluation. The comparison confirms that IRAM is the only framework among the eight reviewed that concurrently addresses all four critical dimensions: AI-based detection, hybrid threat modeling, railway domain specificity, and quantitative resilience measurement. Rahman et al. [10] cover hybrid threats but lack railway specificity and a resilience index; Ibadah et al. [27] address railway systems but omit quantitative resilience measurement; Dosunmu and Ogundele [42] integrate AI detection with hybrid threat modeling yet do not target railway infrastructure nor provide an RI metric.

TABLE I. COMPARISON OF PROPOSED MODEL WITH SELECTED PRIOR WORK

Study	AI Detect.	Hybrid Threats	Railway	RI Metric
Humayed et al. [3]	Partial	No	No	No
Ghafouri et al. [25]	No	Partial	Yes	No
Rass et al. [16]	No	Yes	No	No
Ali et al. [35]	Yes (99%)	No	No	No
Rahman et al. [10]	Partial	Yes	No	No
Ibadah et al. [27]	No	Partial	Yes	No
Dosunmu & Ogundele [42]	Yes	Yes	No	No
Proposed	Yes – LSTM, SVM, Isolation Forest, Autoencoder (94.2%)	Yes ($\Phi=3.39$)	Yes	Yes (RI)

V. INTEGRATED ARCHITECTURE

The integrated architecture combines the three simulation components into a unified decision-support framework. The overall risk score S is computed as a weighted combination of the anomaly score $A(x)$, the Hybrid Risk Score HRS, and the resilience deficit $(1 - RI)$, with weights 0.35, 0.40, and 0.25, respectively, calibrated against the relative operational priority of each dimension in a railway CI context. In the AI-driven simulation, anomaly detection provides early warning signals derived from historical attack pattern libraries; scenario modeling estimates likelihood and impact through Monte Carlo simulation over historical input distributions [41]; and resilience evaluation quantifies projected operational consequences using infrastructure performance benchmarks from the literature.

The architecture is designed to satisfy the SMART-PRAGMATIC cybersecurity metrics requirements [11]: each module produces specific, measurable, actionable, and time-dependent outputs from the simulation. Digital management models studied by Dimitrov and Manchev [31] provide the operational data layer feeding into the scenario modeling module. The simulation framework supports three operational modes: (1) continuous background monitoring — where the AI model processes real-time or historical input streams; (2) on-demand hybrid-threat scenario assessment; and (3) post-incident resilience analysis for recovery planning. The current model represents a validated simulation

prototype. Operational deployment would require integration with live data streams, system-specific calibration, and formal certification in accordance with sectoral standards such as IEC 62443 and CLC/TS 50701, as well as alignment with the national requirements set out in the Bulgarian Cybersecurity Act [38].

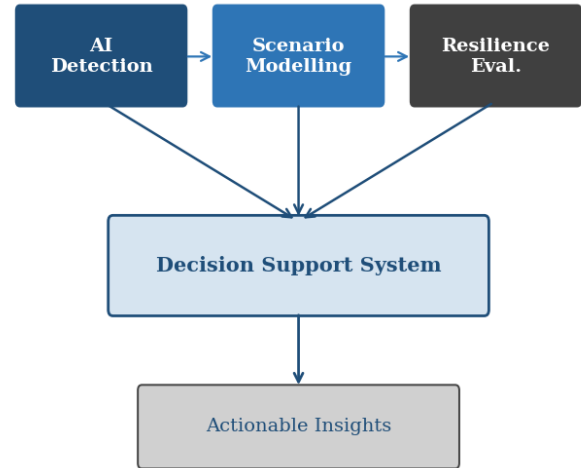


Fig. 7. Integrated IRAM architecture encompassing detection, modeling, resilience, and decision support.

VI. CONCLUSIONS

The study introduces an Integrated Risk Assessment Model (IRAM) that unifies AI-based anomaly detection, hybrid-threat modeling, and resilience analysis into a single composite score S . Simulation results demonstrate **94.2% detection accuracy**, an **87% reduction in false negatives**, a hybrid-threat amplification factor of $\Phi = 3.39$, and a Resilience Index decline to **0.71–0.79**. None of the eight frameworks reviewed in Table I simultaneously covers all four dimensions — a gap that has practical consequences for operators required to demonstrate quantified resilience under NIS2.

The amplification factor $\Phi = 3.39$ is the most operationally significant result: it means a combined cyber-physical attack carries roughly 3.4 times the risk of an equivalent isolated intrusion. This is not a marginal difference — it changes the category of response required. Automated detection within the 15-second anomaly window is therefore not a desirable feature but a functional requirement. The RI drop to 0.71–0.79 under attack conditions translates to a recovery time increase of up to 260% — from 4 minutes to 11–17 minutes. For a busy passenger corridor, that window determines whether a delay becomes a disruption or a crisis.

Three extensions are planned: adaptation of IRAM to metro and port logistics contexts, integration with live SCADA data streams from a Bulgarian railway pilot, and an automated response layer using transfer learning to reduce recalibration time when threat patterns shift [47].

The escalation dynamics documented here suggest that NIS2 minimum standards, while necessary, are not sufficient for high-density rail networks. Regulators would

strengthen compliance frameworks by adding a quantitative resilience floor — an RI threshold below which an operator cannot be certified as operationally secure [37].

VII. ACKNOWLEDGMENTS

The authors declare no funding or conflicts of interest relevant to this study.

VIII. REFERENCES

- [1] ENISA, “Railway cybersecurity: Good practices and recommendations,” EU Agency for Cybersecurity, Heraklion, Greece, Tech. Rep., 2021. [Online]. Available: <https://www.enisa.europa.eu>. Accessed: Apr. 2026.
- [2] UIC, “Cybersecurity for rail digital transformation,” Int. Union of Railways, Paris, France, Tech. Rep., 2020. [Online]. Available: <https://uic.org>. Accessed: Apr. 2026.
- [3] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security—a survey,” *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, 2017. <https://doi.org/10.1109/JIOT.2017.2703172>
- [4] M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” *IEEE Trans. Ind. Inform.*, vol. 9, no. 1, pp. 277–293, 2013. <https://doi.org/10.1109/TII.2012.2198666>
- [5] IMARC Group, “Railway Cyber Security Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2026–2036,” IMARC Group, New York, Tech. Rep., 2024. [Online]. Available: <https://www.imarcgroup.com/railway-cyber-security-market>
- [6] UniDatos Market Insights, “Railway Cybersecurity Market: Current Analysis and Forecast (2024–2032)” [Eisenbahn-Cybersecurity-Markt: Aktuelle Analyse und Prognose (2024–2032)], UniDatos, Tech. Rep., Apr. 2025. [Online]. Available: <https://unidados.com/de/reports/railway-cybersecurity-market>. Accessed: Apr. 2026.
- [7] M. Yilmaz et al., “Non-local attention enhanced deep learning for robust cyberattack detection in industrial IoT-based SCADA systems,” *Scientific Reports*, vol. 16, no. 1, 2026, Art. no. 37146, <https://doi.org/10.1038/s41598-026-37146-1>.
- [8] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, Melbourne, VIC, Australia, 2011, pp. 4490–4494, <https://doi.org/10.1109/IECON.2011.6120048>.
- [9] E. Luijck, M. Klaver, and A. Nieuwenhuijs, “Empirical findings on critical infrastructure dependencies in Europe,” in *Critical Information Infrastructure Security (CRITIS 2008, Lect. Notes Comput. Sci.*, vol. 5508), R. Setola and S. Geretshuber, Eds. Berlin: Springer, 2009, pp. 3–14. https://doi.org/10.1007/978-3-642-03552-4_28
- [10] U. Rahman, H. Ahmed, M. R. I. Khan, M. Saqlain, S. A. Siddiqui, and S. Akhtar, “Comprehensive cybersecurity risk assessment framework for industrial control systems (ICS) and SCADA environments: Identifying threats, vulnerabilities, and mitigation strategies,” *Global Res. J. Nat. Sci. Technol.*, vol. 3, no. 3, pp. 134–153, 2025. <https://doi.org/10.53762/grjnst.03.03.07>
- [11] W. K. Brothby and G. Hinson, *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. Boca Raton, FL: CRC Press/Auerbach Publications, 2013. ISBN 978-1-4398-8152-0. <https://doi.org/10.1201/b14047>
- [12] M. M. Taaama, “Security for Cyber-Physical Systems Using Machine Learning-Based Anomaly Detection: A Survey,” Zenodo [Preprint], 2024. <https://doi.org/10.5281/zenodo.13369313>.
- [13] DataGuard, “Risk Mitigation and Risk Minimization: Protection Against Cyber Threats” [Risk Mitigation & Risikominimierung: Schutz vor Cyberbedrohungen], DataGuard Blog, 2024. [Online]. Available: <https://www.dataguard.de/blog/risk-mitigation-und-risikominimierung/>. Accessed: Apr. 2026.
- [14] Riskconnect, “The Role of Cybersecurity Risk Assessment Software in Mitigating Cyber Threats,” Riskconnect IT Risk Management Blog, 2024. [Online]. Available: <https://riskconnect.com/it-risk-management/the-role-of-cybersecurity-risk-assessment-software-in-mitigating-cyber-threats/>
- [15] F. Flammini, Ed., *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction*. Cham, Switzerland: Springer International Publishing, 2019. <https://doi.org/10.1007/978-3-319-95597-1>
- [16] S. Rass, S. Schauer, S. König, and Q. Zhu, *Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*. Cham, Switzerland: Springer International Publishing, 2020. <https://doi.org/10.1007/978-3-030-46908-5>
- [17] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, “Cybersecurity testbeds for industrial control systems,” *IEEE Security & Privacy*, vol. 11, no. 4, pp. 36–44, 2013. doi: 10.1109/MSP.2013.49.
- [18] C. Wang, N. Du, and H. Yang, “Generation and Analysis of Attack Graphs,” *Procedia Eng.*, vol. 29, pp. 4053–4057, 2012. <https://doi.org/10.1016/j.proeng.2012.01.618>
- [19] Cyble, “Cyber Threats Surge Against Maritime Industry in 2025,” Cyble Research and Intelligence Labs, Jul. 2025. [Online]. Available: <https://cyble.com/blog/cyberattacks-targets-maritime-industry/>
- [20] Industrial Cyber, “Hacktivists, nation-state hackers target global maritime infrastructure as cyberattacks, GPS spoofing surge,” Industrial Cyber, Jul. 2025. [Online]. Available: <https://industrialcyber.co/transport/hacktivists-nation-state-hackers-target-global-maritime-infrastructure-as-cyberattacks-gps-spoofing-surge/>
- [21] CNN Business, “European air traffic control says attack by pro-Russian hackers not affecting flights,” CNN, Apr. 21, 2023. [Online]. Available: <https://www.cnn.com/2023/04/21/business/eurocontrol-russia-hackers/>
- [22] EUROCONTROL, “Air Traffic Management: A Cybersecurity Challenge,” EUROCONTROL, Brussels, Belgium, Tech. Rep., Dec. 2021. [Online]. Available: <https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf>. Accessed: Apr. 2026.
- [23] P. Marks, “Russia hacked an American satellite company one hour before the Ukraine invasion,” MIT Technology Review, May 10, 2022. [Online]. Available: <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>
- [24] SEC Consult, “Cyber Threats to Public Charging Infrastructure: Risks and Protective Measures Through Penetration Testing” [Cyber-Bedrohungen für die öffentliche Ladeinfrastruktur: Risiken und Schutzmaßnahmen durch Penetrationstests], SEC Consult Blog, Jan. 2025. [Online]. Available: <https://sec-consult.com/de/blog/detail/cyber-bedrohungen-fuer-die-oeffentliche-ladeinfrastruktur-risiken-und-schutzmassnahmen-durch-penetrationstests/>. Accessed: Apr. 2026.
- [25] M. Ghafouri et al., “Online Recursive Detection and Adaptive Fuzzy Mitigation of Cyber-Physical Attacks Targeting Topology of IMG: An LFC Case Study,” *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 2129–2145, Mar. 2024. <https://doi.org/10.1109/TSG.2023.3304537>
- [26] M. Maranco et al., “Cyber Security for Intelligent Transportation Systems Protecting Critical Infrastructure,” in *Urban Mobility and Challenges of Intelligent Transportation Systems*, K. Bellam et al., Eds. IGI Global Scientific Publishing, 2025, pp. 403–420. <https://doi.org/10.4018/979-8-3693-7984-4.ch022>
- [27] N. Ibadah, C. Benavente-Peces, and M.-O. Pahl, “Securing the future of railway systems: A comprehensive cybersecurity strategy for critical on-board and track-side infrastructure,” *Sensors*, vol. 24, Art. no. 8218, Dec. 2024. <https://doi.org/10.3390/s24248218>
- [28] E. Pencheva, I. Atanasov, and V. Trifonov, “Identity Management in Future Railway Mobile Communication System,” *Appl. Sci.*,

- vol. 12, no. 9, Art. no. 4293, Apr. 2022. [Online]. Available: <https://doi.org/10.3390/app12094293>
- [29] H. Hindy et al., "A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 104650-104675, 2020, <https://doi.org/10.1109/ACCESS.2020.3000179>
- [30] Z. Wang et al., "Explaining the Attributes of a Deep Learning Based Intrusion Detection System for Industrial Control Networks," *Sensors*, vol. 20, no. 14, Art. no. 3817, 2020, <https://doi.org/10.3390/s20143817>
- [31] D. Dimitrov and I. Manchev, "Methodological and technical aspects of models for digital management of transport systems," *Environment. Technology. Resources*, vol. 1, pp. 39-44, 2024, <https://doi.org/10.17770/etr2024vol2.8049>
- [32] I. S. Stankov, A. P. Aleksieva-Petrova, and G. K. Hristov, "CyberAttacks and Artificial Intelligence: A Systematic Mapping," in *Proc. 2023 Intl. Scientific Conf. on Computer Science (COMSCI)*, Sozopol, Bulgaria, Nov. 2023, pp. 1-7, <https://doi.org/10.1109/COMSCI59259.2023.10315929>
- [33] Z. Wang and X. Liu, "Cyber security of railway cyber-physical system (CPS) – A risk management methodology," *Communications in Transportation Research*, vol. 2, 2022, Art. no. 100078, <https://doi.org/10.1016/j.commtr.2022.100078>
- [34] D. Dimitrov, P. Zlateva, and D. Velev, "A methodology for designing an information system for road infrastructure monitoring," *IOP Conf. Ser.: Earth Environ. Sci.*, vol. 167, no. 1, Art. no. 012044, 2018, <https://doi.org/10.1088/1755-1315/167/1/012044>
- [35] S. M. Ali, A. Razzaque, H. Abbass, M. Yousaf, and S. S. Ali, "A novel AI-based integrated cybersecurity risk assessment framework and resilience of national critical infrastructure," *IEEE Access*, Early Access, 2024, <https://doi.org/10.1109/ACCESS.2024.3524884>
- [36] "Public Transport Act" [Закон за обществения транспорт], *State Gazette (D.V.)*, no. 32, 2026. [Online]. Available: <https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=242220>. Accessed: Apr. 2026.
- [37] European Parliament and Council of the EU, "Directive (EU) 2022/2555 (NIS 2 Directive)," *Official Journal of the EU*, L 333, pp. 80-152, Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [38] "Cybersecurity Act (2018), as amended in State Gazette no. 17, 13 Feb. 2026" [Закон за киберсигурността (2018), изм. и доп. ДВ бр. 17 от 13 февруари 2026 г.]. [Online]. Available: <https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=241234>. Accessed: Apr. 2026.
- [39] D. Abshari and M. Sridhar, "A survey of anomaly detection in cyber-physical systems," submitted for publication, 2025.
- [40] D. Bhamare et al., "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, Art. no. 101677, Feb. 2020, <https://doi.org/10.1016/j.cose.2019.101677>
- [41] M. Ibrahim et al., "Attack Graph Implementation and Visualization for Cyber Physical Systems," *Processes*, vol. 8, Art. no. 12, 2020, <https://doi.org/10.3390/pr8010012>
- [42] A. A. Dosunmu and P. O. Ogundele, "Integrated threat intelligence automation and simulation models for next generation cyber defense," *Engineering and Technology Journal*, vol. 11, no. 1, pp. 8451-8462, 2026, <https://doi.org/10.47191/etj/v11i01.05>
- [43] B. S. Ntsiepdjap, "Dynamic risk assessment for critical infrastructures under attack," *Int. J. Adv. Res.*, vol. 10, no. 9, pp. 868-908, 2022, <https://doi.org/10.21474/IJAR01/15433>
- [44] D. Dimitrov and K. Lalov, "Intelligent rail transport management systems—methodological essence, goals and tasks," *Environment. Technology. Resources*, vol. 2, pp. 33-38, 2024, <https://doi.org/10.17770/etr2024vol2.8050>
- [45] S. Gatlan, "Cyber Partisans hacktivists claim credit for cyberattack on Belarusian Railways," *The Record from Recorded Future News*, Jan. 24, 2022. [Online]. Available: <https://therecord.media/cyber-partisans-hacktivists-claim-credit-for-cyberattack-on-belarusian-railways>
- [46] T. Starks, "Belarusian hacktivist group attacks Belarusian Railways as military frictions mount," *CyberScoop*, Jan. 24, 2022. [Online]. Available: <https://cyberscoop.com/cyber-partisans-belarus-russia-ukraine/>
- [47] Y. Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 10, pp. 1345-1359, 2010, <https://doi.org/10.1109/TKDE.2009.191>

A Methodology for Strategic Defense Review and its Governance System. (Prototype)

Ivo G. Radulov

Rakovski National Defense College
Defense Advanced Research Institute
Sofia, Bulgaria
i.radulov@rmdc.bg

Abstract—This article is part of a series describing the capability-based defense planning model. This model has been adopted as the primary methodology for conducting Strategic Defense Reviews in the Republic of Bulgaria. The proposed prototype for conducting strategic defense reviews follows a sequence of abstract steps to achieve adequate defense capabilities for the armed forces. The article focuses on the planning process within the Ministry of Defense and the Bulgarian Army and includes a model of the activities, information flows and links, and other elements of the process. The activities of the planning process are decomposed to the third level, which completes the design of the system. The functions of the participants in the process and their responsibilities at the various levels of management are described.

The proposed methodology is based on modern scientific and analytical methods. It was validated during the Strategic Defense Review conducted in 2019.

Keywords— Strategic Defense Review, Defense Planning, Model of a Complex Organizational System, Process Modeling.

I. INTRODUCTION

The achievement of the planned level of effectiveness of defense decisions related to the development of the necessary defense capabilities depends to a significant extent on and is determined by high-quality defense planning and the implementation of the transformation of the armed forces. This aspect is of particular relevance given the uncertainty of the future security environment. Preserving and developing defense capabilities in response to threats and commitments to national and global security, under conditions of severe constraints on available resources, necessitates the search for adequate methods to enhance the effectiveness of the defense planning process.

The Strategic Defense Review (SDR) is a key process for analyzing the country's defense capabilities in light of current security threats. SDR aim to identify shortcomings and deficiencies, address these weaknesses, and set realistic

goals for enhancing the capabilities of the armed forces so that they meet national and coalition political-strategic requirements. All of this must be done within the framework of available

resources, minimizing the likelihood of spending funds on capabilities that are not essential and do not contribute to

achieving the set goals. In other words, the results of the SDR must present the overall state of defense as part of national security, so that the prospects for its development are outlined in a manner that is understandable and transparent to the public.

The Strategic Defense Review is a complex process, the success of which depends on a number of factors related to the organization of activities, the selection of an appropriate methodology for its conduct, the establishment of procedures, schedules, resources, and conditions for implementing the activities of the defense planning process, and, last but not least, the motivation and preparation of the personnel who will participate in it.

The choice of an appropriate methodology for conducting a Strategic Defense Review was one of the tasks set by the political and military leadership of the Ministry of Defense of the Republic of Bulgaria. For this purpose, the planning approaches most commonly used in NATO member states were examined, known in the literature as: 1) Top-Down planning; 2) Bottom-Up planning; 3) Scenario-based planning; 4) Threat-based planning; 5) Mission-Based planning; 6) Hedging—an approach based on risk reduction or complete risk control; 7) Technological approach; 8) Financial (or “Budget”) approach [1].

Each of these approaches has distinctive features, with their respective strengths and weaknesses.

The process of capability-based defense planning is a variation of some of the approaches listed above. It is a key planning tool that reflects the characteristics of the

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.111>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

contemporary security environment. The goal of this process is to protect and advance national interests by building, maintaining, and utilizing defense capabilities appropriate to the security environment. It is for this reason that the leadership has chosen this approach as the mechanism for conducting the upcoming Strategic Defense Review.

The capability-based defense planning process has been in use at the Ministry of Defense and the Bulgarian Armed Forces since 2012, when a methodological guide for implementing this approach was first developed. The realities of the environment, as well as the results of past strategic defense reviews, have necessitated an analysis of the existing “Capability-Based Defense Planning Guide” from 2012, with the aim of updating and improving it.

As a result of the analysis of the 2012 Planning Guide, a number of shortcomings were identified, including: the lack of regulated relationships between performers; the lack of defined responsibilities for officials; “parasitic” activities that do not add “value” to the defense planning process, incompatibility between national defense planning and NATO capability planning has been restarted. The “Planning” stage of the process was not described, nor was the “Project management” stage; the process activities were not correctly visualized, and the responsibilities of the individuals participating in the process have not been specified.

The main conclusions of the analysis are that the model of activities in the planning process 2012 is inconsistent, incomplete, and does not correspond to the current defense management system. Therefore, in its current form, it cannot be used as a methodology for conducting the future defense review.

With the aim of addressing the identified weaknesses, the model was revised and refined into a “To-Be” model of the future state so that it integrates and reflects all key functional and systemic perspectives of defense management.

The methodology follows the recommendations from an analysis of the existing defense planning system. The identified shortcomings and gaps, primarily related to the lack of compatibility between the specific characteristics of national defense planning and the armed forces and the requirements for NATO collective defense planning, have been addressed. Changes to the regulatory framework (primarily the Ministry of Defense’s Rules of Procedure) related to the duties and responsibilities of officials have also been reflected. Activities have been added for: 1) long-term defense planning; 2) project management; 3) research and development (R&D); 4) life-cycle management. Mechanisms have been established to enhance oversight, ensure the fulfillment of the country’s commitments to NATO and the European Security and Defense Policy (ESDP), and synchronize the planning process with analogous processes in NATO and the EU. The goals, stages, and activities of the process are clearly described using standard notation for process description and visualization. Activities that do not provide real “added” value to the process in terms of enhancing the capabilities

of the armed forces have been optimized, and the relationships between the performers have been redesigned in accordance with their responsibilities.

The methodology presents the process through a series of decomposed activities with their respective inputs, outputs, and participants. Changes have also been made to the names of the process’ elements. The terminology has been refined and standardized. As a result of these changes, a fully completed prototype has been developed, providing a detailed description of the process, products, organizational structure, relationships and responsibilities of officials, to ensure effective integrated planning and capability development in response to the changing operational environment.

The methodology regulates defense planning as a specific activity carried out within the Ministry of Defense, aimed at defining, building, and developing the necessary capabilities and the associated human, financial, material, and other resources and services to achieve defense objectives in fulfillment of the Republic of Bulgaria’s obligations within collective security and defense systems. This prototype presents: 1) defense planning as a process; 2) the logical link between national defense policy and strategic documents related to the country’s national security and defense, and the defense capabilities necessary to achieve the objectives and priorities set forth therein; 3) capability planning activities; 4) the main participants in the process and their responsibilities.

II. MATERIALS AND METHODS

To identify realistic solutions when designing the system architecture, formal methods for description and analysis were employed, including mathematical and logical techniques, as well as descriptive languages and tools for the development and verification of complex systems. These methods and techniques are characterized by a high level of precision, aimed at ensuring the adequacy of the system design and avoiding errors in it. The following main formal methods and tools were used:

- *IDEF0 diagrams.* The activity model was visualized using IDEF0 diagrams. IDEF0 belongs to a family of modeling languages that cover a wide range of applications—from functional modeling to data modeling, simulation, object-oriented analysis/design, and knowledge acquisition. A fundamental principle underlying IDEF0 diagrams is the principle of activity decomposition. Activity decomposition is the breakdown of processes into their constituent activities. The result is a tree-like structure representing the activities required to solve a given problem. The IDEF family integrates methods ranging from IDEF0 to IDEF14 [2]. The figures in this article were created using CASE (Computer-Aided Software Engineering) [3] tools based on the IDEF0 standard.
- A validation of the overall model, with a complete decomposition of the activities, was accomplished using the Visual Object Net++ Evaluation Version 2.0.

- The models presented in the methodology have been examined for completeness and consistency using a separate methodology that includes descriptive and analytical tools such as Evaluation Nets, algorithm flowcharts, tabular algorithm flowcharts, and matrix algorithm diagrams (MAD). An example of this proof is given in [4].

III. RESULTS AND DISCUSSION

METHODOLOGY FOR CONDUCTING A STRATEGIC DEFENSE REVIEW AND THE SYSTEM FOR ITS MANAGEMENT

The methodology presented follows the capability-based defense planning process of the updated To-Be model.

This process is a key planning tool in the contemporary security environment, characterized by extreme dynamism, blurring of boundaries between internal and external security, and broadening of the spectrum of identified threats. The goal of this process is to protect and advance national interests by building, maintaining, and utilizing defense capabilities appropriate to the security environment, and by establishing interoperable, modern armed forces with a unified command and control system in peacetime and during crises [5].

A key stage in the defense planning process is identifying the capabilities that will be required for current and future operations over the next ten to fifteen years. For this reason, operational planning is a primary tool for determining the necessary capabilities. Through this process, the defined national strategic objectives are broken down into military objectives, potential operations, and tasks, which in turn are broken down into the forces and assets required to execute these tasks in operations. Given that “The defense of the Republic of Bulgaria is a system of political, economic, military, social, and other activities aimed at ensuring a stable security environment and at preparing for and carrying out the armed defense of the territorial integrity and independence of the state,” capability-based defense planning, together with the planning and conduct of operations, are systemic determinants of the country’s defense [5].

A. Restrictions

Within the overall capability-based defense planning model, the methodology for conducting Strategic Defense Reviews and the system for managing them focuses on the activities “Formulation of Defense Policy” and “Capability Planning” (Fig. 1). The remaining activities in the process are related to the implementation of decisions from previous strategic reviews or define the input parameters from the previous planning cycle, such as the financial framework, the Government Program, the Current Program for the Development of the Armed Forces, modernization and rearmament projects implemented to date, etc.

B. Assumptions

The methodology has been adapted to the current defense management system, including applicable laws and regulations, and meets the following requirements: 1) to correspond to the strategic plans of the organization, 2) to allow for continuous change and transformation, 3) to provide standard descriptions and a common working environment, 4) the model’s outputs must objectively reflect information flows within the organization, 5) control mechanisms must be established to prevent management from implementing incompatible decisions.

C. Formulation of Defense Policy Stage

Defense policy serves as the starting point for initiating and conducting the defense planning process. Defense policy is a sectoral component of national security policy and constitutes a set of coordinated objectives and institutional and civilian actions aimed at developing, improving, maintaining, and utilizing defense capabilities to protect national interests [5].

The primary objective of defense policy is to create conditions for the optimal use of the armed forces within the context of national security policy, taking into account the strategic security environment, the country’s resource capabilities in the medium term and their projected development in the longer term, and our participation in NATO’s collective defense and the EU’s Common Security and Defense Policy [5].

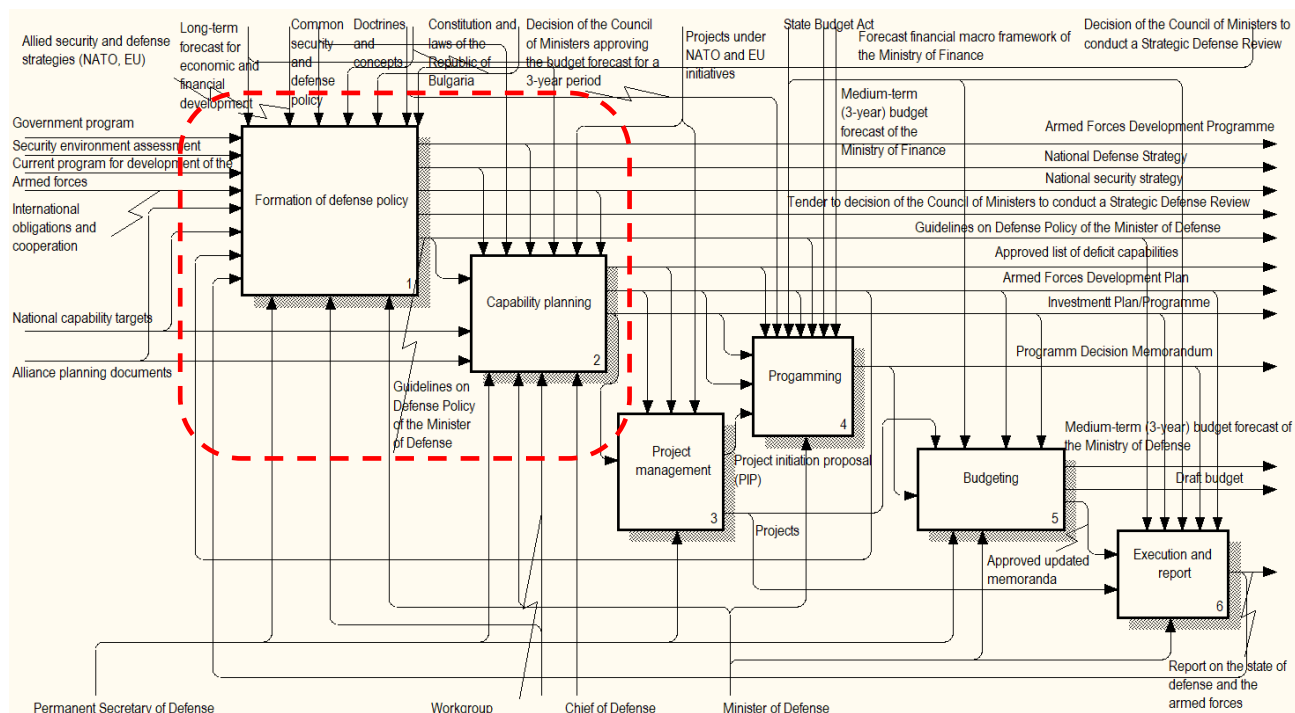


Fig. 1. A0 Model of capability-based defense planning processes

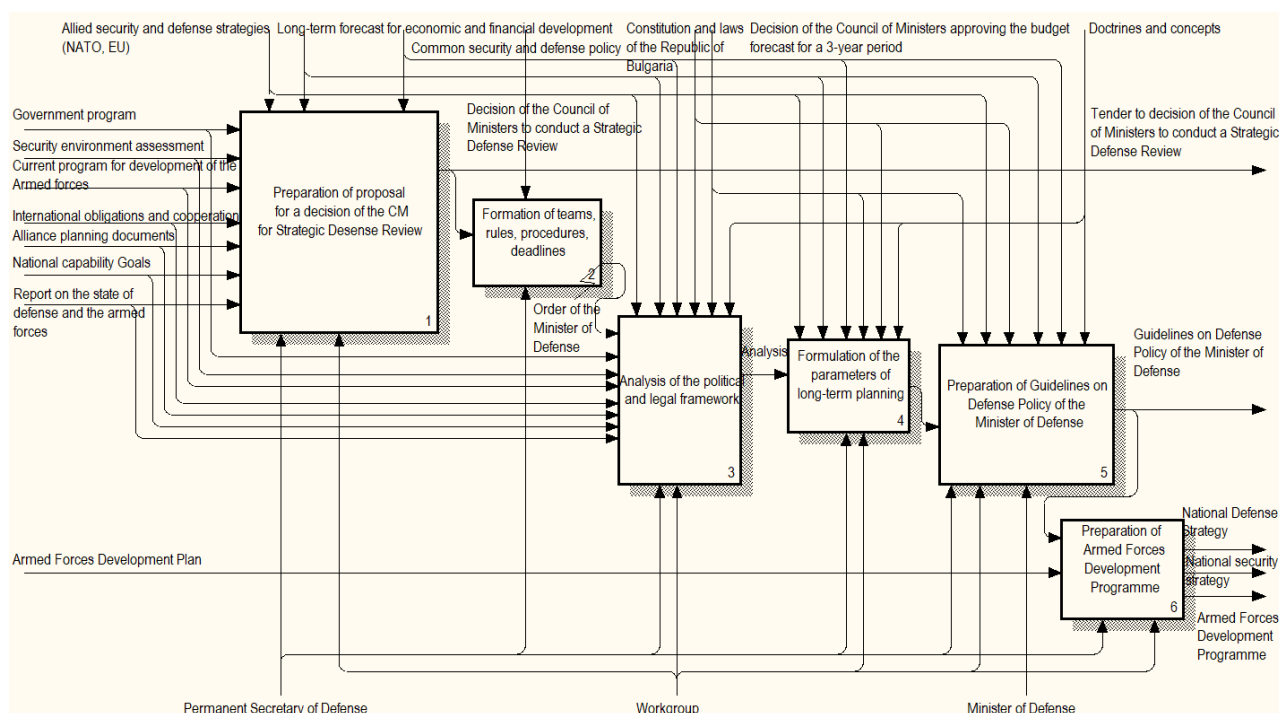


Fig. 2. Stage A1 „Formulation of Defense Policy”

The main deliverables from this stage are: 1) Proposal for decision of the Council of Ministers to conduct a Strategic Defense Review; 2) Guidelines of the Minister of Defense on the Defense Policy; 3) National Defense Strategy; 4) National security strategy; 5) Armed Forces Development Programme (Fig. 2).

A proposal to conduct a new Strategic Defense Review is made prior to the expiration of the relevant planning period or in the event of a change in the security environment.

The Guidelines on Defense Policy serve as the primary framework document in the defense planning process and mark the beginning of a new planning cycle. When conducting a strategic defense review and/or periodic defense reviews, the Minister of Defense issues guidelines for conducting a strategic review and/or defense review. The guidelines include information necessary for the overall planning process, namely: an assessment of the security environment, the level of ambition for the use of the armed forces (AF), the role of the armed forces, defense policy priorities, the titles of the general planning scenarios, an estimated financial framework, strategic planning assumptions, and constraints.

One of the mechanisms for aligning the national defense planning process with the NATO Defense Planning Process is precisely the Guidelines on Defense Policy. Therefore, their development must begin as soon as work starts on drafting the NATO Political Guidance. Another such mechanism is adopted National Capability Goals.

The Armed Forces Development Programme is the primary conceptual, strategic, and programmatic document for national defense, with a long-term nature and a 10–15-year horizon. It defines the parameters for development and the main guidelines for building the defense capabilities of

the armed forces. It aims to achieve broad public and political support, continuity, stability, consistency, and sustainability in the implementation of defense policy and the development of defense capabilities in the long term, beyond the terms of the current government and parliament [5]. The Armed Forces Development Programme contains:

- conclusions from the assessment of the security environment and their impact on the development of defense capabilities;
- foundations of defense policy (principles, strategic objectives, and priorities);
- general requirements for defense capabilities;
- guidelines for the development of the Armed Forces' defense capabilities;
- macro-level resource framework;
- key objectives of defense policy.

Another key document from this stage is the National Defense Strategy. It is updated as necessary during the strategic defense review. The National Defense Strategy is reviewed by the Defense Council (DC) and adopted by the

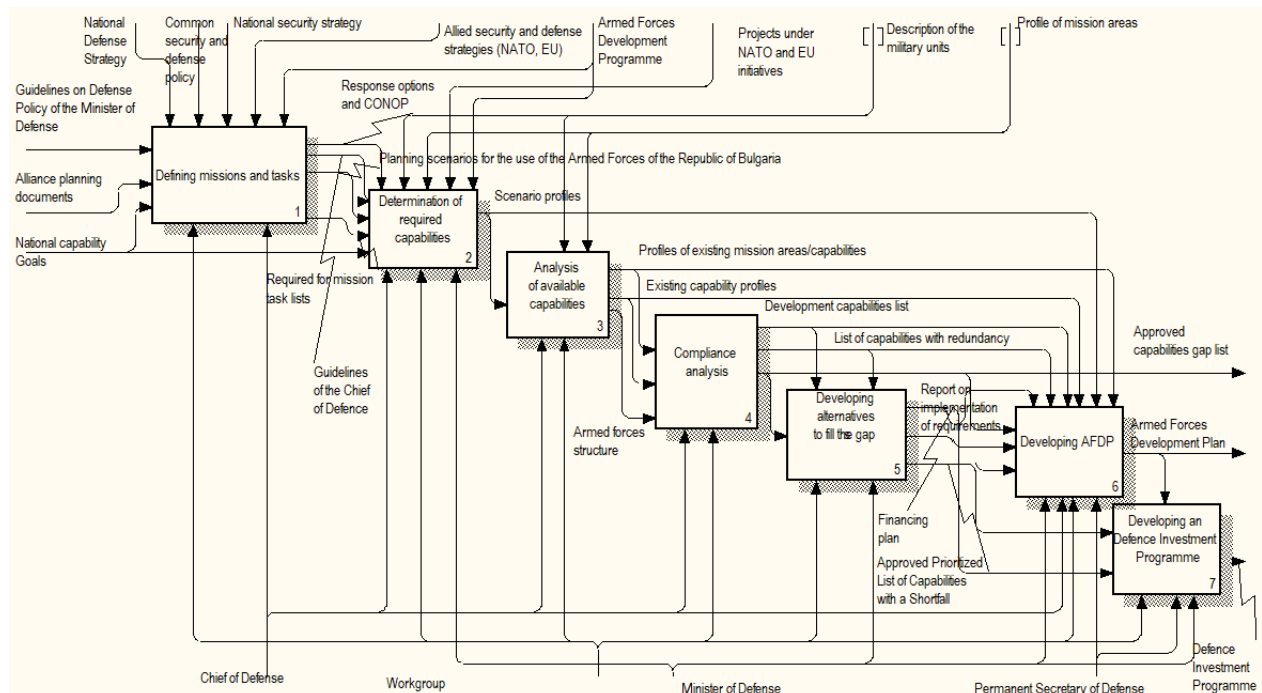


Fig. 3. Stage A2 „Capability Planning”

Council of Ministers upon the recommendation of the Minister of Defense.

D. Capability Planning Stage

In the Capability Planning Stage, changes in the security environment and political decisions are transformed into the capabilities required to achieve

defense objectives. This stage includes the following activities, which are presented in Fig. 3:

1. Defining the missions and tasks of the armed forces;
2. Determination of required capabilities;
3. Analysis of available capabilities;
4. Compliance analysis;
5. Developing alternatives to fill the gaps;
6. Developing an Armed Forces Development Plan (AFDP);
7. Development of Defense Investment Programme.

The essence of this stage is to identify the defense capabilities that will be required over the next 10–15 years and to draw up a plan for their maintenance, development, and acquisition.

This stage is repeated every four years (during strategic or periodic defense reviews) or, if necessary, every two years.

The deliverables of this stage are: 1) Armed Forces Development Plan; 2) Defense Investment Programme; 3) Approved Capabilities Gap List.

The Defense Secretary directly oversees and is responsible for defense planning. At this stage, the Chief of Defense directly oversees and is responsible for determining the necessary defense capabilities, coordinating with the Minister of Defense on the main military-political objectives, military-political scenarios, and the principles under which the country's military and civilian capabilities are used for its effective defense.

1. Defining missions and tasks of the armed forces.

This step aims to identify the capabilities required to achieve defense objectives and fulfill the Republic of Bulgaria's obligations within the collective security and defense system. It includes the following activities [5]:

- developing directives from the Chief of Defense;
- developing planning scenarios;
- developing courses of action and concepts of operations;
- development of task lists.

The required capabilities are defined as the capacity to perform the tasks/actions necessary to achieve the objectives of potential operations in response to probable threats and in fulfillment of the Republic of Bulgaria's obligations within the collective security and defense system.

To this end, the threats identified during the security environment analysis are further developed into situational scenarios, based on which response options and operations to be conducted to achieve national objectives are determined. Subsequently, based on existing conceptual and doctrinal documents (guidelines, internal/operational

tactics, techniques, procedures, rules, etc.), the tasks and actions required to carry out these operations are defined.

2. Determination of Required Capabilities.

In this step, the tasks/actions identified for execution are grouped by similarity (by domain) and by the structures (formations) that will execute them within the approved planning scenarios [5].

This step involves:

- developing or updating mission/capability areas;
- defining scenario profiles;
- review by the Defense Capabilities Council (DCC).

3. Analysis of available capabilities.

The analysis of available capabilities is an activity aimed at:

- describing existing capabilities;
- analyzing and assessing the existing structure of the Armed Forces for the execution of tasks in operations.

As a result of these activities, three main documents are developed:

- Profile of existing mission/capability areas;
- Profile of existing capabilities;
- Structure of the Armed Forces

4. Compliance analysis.

The capability assessment includes the following activities [5]:

- identifying areas where existing capabilities are sufficient - These include available capabilities for which (from previous defense reviews or the current Armed Forces Development Programme) a political-military consensus on their development has already been reached and they have been identified as necessary within the current defense planning process. This also includes those capabilities for which the life cycle of weapons, equipment, or systems is set to end within the next ten years. As a result of this list, funds are being planned/budgeted for their maintenance and development;
- Identifying areas where existing capabilities are in surplus. Surplus capabilities include those that are currently available but exceed, in terms of quantity or quality, the levels deemed necessary within the current defense planning process, and capabilities for which weapons, major equipment, or equipment are at the end of their life cycle or for which modernization is not financially feasible to meet the requirements of the tasks being performed. As a result of this list, funds are planned/budgeted for the decommissioning of existing capabilities, the termination of ongoing projects, or the development of new ones;

- Identifying the shortfall in the capabilities required by the Armed Forces to carry out their assigned missions and tasks. This includes capabilities that must be developed because they are not currently available but have been identified as necessary within the current defense planning process. This also includes capabilities that are currently available, but for which weapons, major equipment, or systems are at the end of their life cycle or for which modernization is not financially viable to meet the requirements of the tasks being performed;
- Prioritization of capabilities. Capabilities are prioritized according to their significance for achieving the desired end result within the scenarios and according to a separate methodology [6], which generally defines: the weighting parameters of the required capabilities and the importance parameters of the required capabilities that are in short supply. The output of this stage is a prioritized list of capabilities;
- Approval of the list. The prioritized list of capabilities is developed within three months of the approval of the scenario profiles by a Joint Planning Group, reviewed by the Joint Staff, and approved by the National Security Council.

The Chief of Defense, together with the Secretary of Defense, oversees the implementation of the activities.

5. *Developing alternatives to fill in the gaps.*

The development and selection of options involves the following activities:

- Developing options to address capability gaps. This step identifies the human, financial, material, and other resources and services that will be used to maintain, build, and develop the necessary capabilities. This step marks the transition from capability planning to resource planning, as the identified required capabilities are transferred into required resources and compared with the country's resource capacity to provide them. In this process, the overall financial framework presented in the Defense Policy Guidelines is allocated to support existing capabilities and address capability gaps. The capability shortfall is calculated as the sum of capabilities in deficit and capabilities requiring development (modernization or replacement of weapons, equipment, and materiel).
- Development of detailed options. The various options are further refined by the Joint Planning Group so that they are sufficiently clear to enable the forecasting of the resources required for their implementation. The options are analyzed and refined based on: 1) the availability of resources and 2) the extent to which they can be implemented (politically, militarily, and technologically) to address the relevant capability shortfall within the

required timeframe and to meet the established standards.

- review by the Armaments Council (AC);
- review by the Program Council (PC);
- review by the DCC.

6. *Developing of an Armed Forces Development Plan.*

This stage includes the following activities:

- Development of AFDP. The Armed Forces Development Plan defines: the organizational structure, command and control bodies, chain of command, strength, deployment, armaments, equipment, and material resources of the military units and structures of the armed forces, as well as the voluntary reserve of the armed forces. The Plan covers a ten-year period and is developed, amended, or updated during a defense review (every 4 or 2 years). It is adopted by the Council of Ministers;
- review by the Security Council;
- submission for coordination and approval by the Council of Ministers of the Republic of Bulgaria.

7. *Development of a Defense Investment Programme.*

The Defense Investment Programme (DIP) aims to ensure the acquisition of the "hardware" component of the capabilities outlined in the Armed Forces Development Plan. The DIP is developed largely on the basis of concepts with selected options for addressing capability gaps and forms a unified integrated framework for capital expenditures, including the acquisition, integrated logistics support, decommissioning, and/or modernization of defense equipment, and infrastructure, through the implementation of investment, infrastructure, international, and other projects.

The DIP covers a ten-year period and is developed, amended, or updated during a defense review (every 4 or 2 years) or as necessary—by decision of the Minister of Defense.

The Chief of Defense, together with the Secretary of Defense, leads and is responsible for the development of the DIP.

The Armed Forces Development Plan and the Defense Investment Programme are the final products of the Capability Planning Phase and serve as the primary documents for the subsequent phases. All actions within the accompanying Project Management Process and the Programming, Budgeting, and Implementation and Reporting Phases should ensure the implementation of these two documents.

IV. · CONCLUSIONS

Capability planning is a process for the acquisition, development, or phasing out of defense capabilities in

response to changes in the security environment. This approach is fundamental to national defense. The proposed prototype methodology for conducting strategic defense describes the sequence of activities aimed at achieving adequate defense capabilities for the armed forces in peacetime. The methodology was used during the Strategic Defense Review conducted in 2019. Thus, the model was validated. The following criteria were used to validate the methodology: 1) Quality and Compliance criteria and 2) Performance Metrics

During the Strategic Defense Review, the model demonstrated stability, and the process activities were carried out within the defined parameters without significant deviations. The methodology met the predefined specifications and regulatory standards, i.e., it proved to be practically applicable. The ability to repeat the process multiple times with consistent quality results was demonstrated, which is evidence that the proposed model is reproducible.

As a result of the review, using the proposed methodology, 188 minimum required military capabilities were identified and prioritized in a list of capability gaps. After accounting for the necessary and available financial resources, these capabilities were optimized to 38. Thus, in practice, the optimal, compromise option was determined within the given financial resources, through which all formations declared in NATO's Capability Goals and initiatives can be established, as well as the critically important capabilities related to the implementation of the three main projects for the rearmament of the Armed Forces at that time. In practice, all final states has been reached.

Despite the mechanisms built into the model to prevent subjective intervention, including: regulatory clarity and predictability, detailed descriptions of procedures and activities, the creation of clear algorithms for action that leave no scope for interpretation, the establishment of principles of "bound competence", the implementation of organizational and control mechanisms, the use of digitization, specialized software, a scientific approach, etc., a lack of integrity, ethical and moral standards, the presence of political affiliations, personal preferences, or prejudices can regulate the results outside the defined framework of the methodology. However, this is characteristic of almost every complex organizational system and can hardly be sufficiently characterized as a shortcoming of the methodology.

The proposed methodological prototype yields good results in peacetime defense planning. Capability planning in wartime is the process of identifying and maintaining the military resources necessary for the effective execution of

combat missions. Essentially, this type of planning must ensure flexibility and an adequate rapid response for the acquisition of defense capabilities and the transformation of defense structures. In wartime, it is logical that some of the activities described in the prototype be reduced to the following:

- Identification of critical capabilities: Focus on intelligence, combat power, air and missile defense, logistics, and cyber defense;
- Gap Analysis: Comparison between the current state and the requirements for actual combat operations;
- Mobilization readiness: Planning for the rapid deployment of human resources;
- War-time economy: Redirecting civilian industry toward military production. The goal is to strengthen defense capacity through defense products, technologies, and dual-use items.

ACKNOWLEDGMENT

The document was developed under the National Scientific Programme "Security and Defense ", funded by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

REFERENCES

- [1] Tagarev, T. Defence and Armed Forces Planning Methodology, Available: https://procon.bg/system/files/2.1_planning_methodology_0.pdf [Accessed May 05, 2026]
- [2] https://www.idef.com/idefo-function_modeling_method/
- [3] Coronel, Carlos; Morris, Steven (February 4, 2014). Database Systems: Design, Implementation, & Management. Cengage Learning. pp. 695–700. ISBN 978-1285196145. Retrieved 25 November 2014.
- [4] Radulov I., Modelling of Capability-Based Defence Planning Processes Print ISSN 1691-5402 Online ISSN 2256-070X Available: <https://doi.org/10.17770/etr2024vol4.8214> [Accessed May 05, 2026]
- [5] Guidelines for capability-based defence planning, introduced for implementation by order of the Minister of Defense № OX-323/29.03.2019.
- [6] Neno Hristov, Ivo Radulov, Petko Iliev, Plamena Andreeva "Prioritization Methodology for Development of Required Operational Capabilities", "SYSTEM ANALYSIS & STUDIES PANEL", SAS-081/RSY, NATO Research and Technology Agency (RTA), 26-28 April 2010, Sofia, Bulgaria. Available: <https://pdfs.semanticscholar.org/73dc/d76478a67e70d27fa3187a068fc23fa36f01.pdf> [Accessed May 05, 2026]

Efficient and Trustworthy Anti-Corruption AI: Leveraging Model Pruning for Secure Deployment in Critical Systems

Tamara Ristovska
Computer Science
University of Library Studies and
Information Technologies
Sofia, Bulgaria
t.ristovska@unibit.bg
ORCID: [0009-0005-9870-1327](https://orcid.org/0009-0005-9870-1327)

Lyubomir Gotsev
Computer Science
University of Library Studies and
Information Technologies
Sofia, Bulgaria
l.gotsev@unibit.bg
ORCID: [0000-0002-5217-5780](https://orcid.org/0000-0002-5217-5780)

Genadiy Gospodinov
Computer Science
University of Library Studies and
Information Technologies
Sofia, Bulgaria
g.gospodinov@unibit.bg
ORCID: [0009-0007-0792-2162](https://orcid.org/0009-0007-0792-2162)

Jordan Deliversky
National Security
University of Library Studies and
Information Technologies
Sofia, Bulgaria
j.deliversky@unibit.bg
ORCID: [0000-0001-7799-1461](https://orcid.org/0000-0001-7799-1461)

Stanislava Cholova
Public Communications
University of Library Studies and
Information Technologies
Sofia, Bulgaria
s.cholova@unibit.bg
ORCID: [0000-0002-5217-5780](https://orcid.org/0000-0002-5217-5780)

Abstract— Corruption in public procurement, financial transactions, and administrative processes presents substantial threats to national and international security, compromising integrity in defense logistics, resource distribution, and governance frameworks. Artificial Intelligence (AI), particularly machine learning models for anomaly detection, fraud identification, and risk prediction, has emerged as a powerful analytical tool for procurement risk monitoring. However, large-scale AI models face significant barriers to deployment in secure, resource-constrained environments such as edge devices used for military or public-sector monitoring. These barriers include high computational demands, susceptibility to adversarial perturbations, and limited interpretability — all of which reduce their suitability for security-critical applications. This study examines model pruning techniques, including structured and unstructured pruning as well as magnitude-based and lottery ticket hypothesis-inspired approaches, to create compact and efficient anti-corruption AI models with minimal accuracy degradation. These pruned models achieve faster inference and substantially reduced memory footprints, enabling deployment on edge devices and in resource-constrained secure environments. Experimental results demonstrate effective identification of key procurement risk signals, including single-bid awards, suspiciously short tender windows, and irregular fund flows. The proposed approach offers a pathway for integrating compact, efficient procurement anomaly detection models into defense and security technologies, supporting decision support systems and infrastructure protection. This work

bridges advances in artificial intelligence with secure technology development, contributing to enhanced societal integrity and resilience.

Keywords— *anti-corruption AI, machine learning, model pruning, procurement anomaly detection.*

INTRODUCTION

Corruption in government procurement, financial management, and administrative systems remains a persistent problem driven by insufficient oversight, low transparency, and inadequate enforcement. Defense logistics and infrastructure development are among the most heavily affected sectors. High-value contracts with limited transparency generate risks that can lead to procurement of substandard equipment, inflated costs, and compromised supply chains, directly undermining operational readiness and national defense capabilities [1], [2]. Recent analyses highlight that accelerated defense spending further amplifies these vulnerabilities, as rapid procurement processes often bypass robust oversight [3]. Defense procurement is frequently identified as one of the highest-risk sectors for corruption due to secrecy requirements, large contract values, and complex technical specifications [4], [5]. In conflict-affected or high-spending environments, such weaknesses not only erode public trust and economic efficiency but also enable foreign influence

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.167>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

and weaken overall security infrastructure [6]. As governments increasingly rely on digital procurement platforms and large-scale data systems, opportunities emerge to leverage advanced analytical tools to detect and mitigate such corruption risks proactively.

The application of AI and machine learning (ML) techniques to anomaly and fraud detection within the public procurement domain has demonstrated strong potential. ML models can analyze and process large volumes of tender data to identify red flags such as single-bid awards, abnormally short tender periods, repeated buyer-supplier relationships, supplier concentration, and irregular pricing patterns. Recent studies show that data-driven approaches — including ensemble methods, unsupervised anomaly detection, and network analysis — have performed successfully on procurement datasets for detecting collusion and favoritism [6], [7]. These systems enable scalable, proactive risk assessment and support integrity efforts in governance and defense-related procurement [8]. However, deploying large AI models to secure, resource-constrained environments like edge devices for real-time surveillance in different kinds of sector settings presents significant challenges. Neural networks typically demand significant processing power and energy, making them unsuitable for execution on edge devices due to their speed and power consumption. They are also susceptible to attacks where minor perturbations to input data can reduce prediction accuracy, a scenario that is undesirable for security-critical environments [9], [10]. Finally, the opaque nature of large models reduces their trustworthiness in contexts such as defense and anti-corruption, where transparent explanations of model behavior are essential.

A critical research gap therefore exists: the need for compact, efficient, and trustworthy anti-corruption AI models capable of secure deployment on edge devices in critical systems. While traditional large-scale models achieve good predictive performance, they rarely satisfy the strict constraints of low memory footprint, fast inference, and adversarial resilience required in defense and security operations.

Model pruning techniques provide a practical solution. Structured and unstructured magnitude pruning, along with methods inspired by the Lottery Ticket Hypothesis, allow removal of redundant parameters while largely preserving accuracy. These approaches significantly reduce model size and computational demands, enabling efficient execution on resource-limited hardware with minimal performance loss [11], [12].

In this study, we apply multiple pruning strategies to an enhanced Multi-Layer Perceptron (MLP) for procurement anomaly detection using real data from the Tenders Electronic Daily (TED) database, with a focus on Bulgarian records from 2023. Anomaly labels are generated through weak supervision based on established procurement red flags documented in anti-corruption literature. We evaluate structured magnitude pruning, unstructured magnitude pruning, and Lottery Ticket-inspired pruning across different sparsity levels. Performance is assessed using

classification metrics (accuracy, F1-score, AUC), efficiency indicators (model size, compression ratio, inference latency), adversarial robustness (via FGSM perturbations), and interpretability (permutation importance).

The main research questions addressed are: (1) Can model pruning maintain or improve predictive performance on weakly supervised procurement anomaly detection while substantially reducing model size and computational cost? (2) How well do pruned models improve practical edge-deployment proxies (memory footprint, latency, quantized size) while retaining robustness under adversarial perturbations?

The remainder of the paper is structured as follows. The Materials and Methods section describes the TED dataset, weak labeling approach, model architecture, and pruning strategies. Results and Discussion present the experimental outcomes, efficiency gains, robustness analysis, and implications. Finally, Conclusions summarize key findings and suggest directions for future work.

I. MATERIALS AND METHODS

A. Related Work

AI and ML methods are more and more used to detect risk of fraud, collusion and corruption in public procurement. Some works use ensembles of ML methods, random forest, Light Gradient Boosting Machine (LightGBM) and unsupervised anomaly detection techniques to identify different anomaly like bid-rigging, favoritism and abnormal prices on huge data sets of tenders [13], [7], [14]. Some frameworks on explainable AI, applied on the Tenders Electronic Daily (TED) database show good performance in the detection of awards and the analysis of local vs non-local winners [7]. Other papers use a combination of machine learning methods and risk indices for a prioritization of surveillance on different indicators, such as costs and delivery delays, highlighting inefficiencies in these indicators [15]. AI is also used by OECD reports, on a support role, to make advance risk assessments and identify non-competitive practices [8]. Model compression techniques are essential for deploying such models in resource-constrained or security-critical environments. Pruning methods, including structured and unstructured magnitude-based pruning, reduce model size and computational demands while aiming to preserve accuracy. Structured pruning removes entire neurons, channels, or filters, enabling hardware-friendly compression suitable for edge devices. Unstructured pruning, by contrast, eliminates individual low-magnitude weights, achieving higher sparsity but often requiring specialized inference engines. Approaches inspired by the Lottery Ticket Hypothesis identify sparse, trainable subnetworks within dense models that can match or exceed original performance after retraining from appropriate initializations [8], [8], [8]. Quantization is sometimes combined with pruning to further reduce memory and latency, though it was not the primary focus of the present work.

Public procurement datasets like TED pose specific challenges for supervised learning: they lack ground-truth corruption labels. Researchers therefore frequently adopt weakly supervised or unsupervised anomaly detection strategies, relying on rule-based red flags or statistical proxies for labeling [8], [8]. While effective for scaling to large volumes of data, these approaches introduce noise and limit direct evaluation against confirmed corruption cases. Most existing studies either use synthetic data, small labeled subsets, or focus solely on predictive accuracy without addressing deployment constraints such as model size, inference speed, or adversarial robustness in secure settings.

The present work addresses these gaps by using real TED data, applying weak supervision based on established anti-corruption red flags, and systematically evaluating pruning strategies with a focus on efficiency, adversarial robustness, and interpretability — aspects critical for trustworthy deployment in defense and security-related monitoring systems.

B. Dataset and Preprocessing

The dataset used in this study consists of real public procurement records extracted from the Tenders Electronic Daily (TED) database, the official EU platform for publishing public procurement notices. TED provides comprehensive, publicly available data on tenders across EU member states and beyond. This work focuses exclusively on Bulgarian procurement-related records for the period from January 1, 2023, to December 31, 2023 — the latest full year with validated CSV coverage at the time of extraction. After cleaning and preprocessing, the final dataset contained 534 records with 111 engineered features. The relatively small size of the dataset was addressed through Dropout regularization, early stopping, and Batch Normalization in the model architecture, all of which mitigate overfitting. Results should be interpreted as a proof-of-concept, and generalizability to other countries or time periods require validation on larger, more diverse datasets.

Because TED does not provide explicit ground-truth labels for corruption or anomalies, a weak supervision approach was employed. Anomaly labels (**is_anomalous**) were generated using a rule-based scoring system derived from procurement red flags widely documented in anti-corruption and public procurement risk literature. Key red flags included

- Single-bid or low-competition awards ($\text{numbers_offers} \leq 1$)
- Abnormally short tender submission windows
- Repeated buyer-supplier relationships
- High supplier concentration
- Price spikes or anomalies relative to historical or market benchmarks
- Irregular fund-flow proxies
- Higher-risk procurement procedures

These indicators were aggregated into a continuous **weak_label_score**. The score was then thresholded to produce the binary target variable **is_anomalous**, resulting in an anomaly rate of approximately 57.49%. Each flag was assigned a weight reflecting its severity as documented in anti-corruption literature: **flag_short_tender_window** (1.5), **flag_single_bid_win** (1.5), **flag_irregular_fund_flow** (1.5), **flag_supplier_concentration** (1.0), **flag_repeated_buyer_supplier** (1.0), **flag_price_spike** (1.0), and **flag_high_risk_procedure** (0.5). The continuous **weak_label_score** was computed as the weighted sum of all active flags for each record. The binary target **is_anomalous** was set to 1 when **weak_label_score** ≥ 3.0 , corresponding to contracts exhibiting at least two mid-weight flags or one high-weight flag combination. This threshold aligns with OECD procurement risk-scoring conventions and was validated against the empirical score distribution in the dataset, where 3.0 represents the 43rd percentile — producing a moderately conservative labeling. It is important to note that this setup defines a weakly supervised procurement risk-detection task rather than a fully supervised corruption classification problem. The approach follows established practices for leveraging domain knowledge when ground-truth labels are unavailable [8].

Feature engineering transformed raw TED fields into 111 predictive variables, including normalized contract values, logarithmic transformations (**log_contract_value**), temporal features (**day_of_week**, **year**), procedural indicators, and relational metrics between buyers and suppliers.

C. Model Architecture and Pruning Strategies

An enhanced Multi-Layer Perceptron (MLP) served as the baseline classifier. The network consisted of fully connected layers with Rectified Linear Unit (ReLU) activations, Batch Normalization, and Dropout regularization to mitigate overfitting on the relatively small dataset. Given the dataset size (534 records), a stratified hold-out split was used rather than k-fold cross-validation, as the latter would result in very small training folds for the pruning fine-tuning stage; this trade-off is explicitly acknowledged as a limitation.

Three pruning strategies were evaluated to create lightweight versions suitable for deployment:

1. Structured magnitude pruning: Removes less important neurons or units in a structured manner.
2. Unstructured magnitude pruning: Eliminates individual weights with the lowest absolute magnitudes while preserving the original architecture.
3. Lottery Ticket Hypothesis-inspired pruning: Identifies sparse subnetworks (“winning tickets”) by iterative magnitude pruning followed by fine-tuning of the remaining weights.

Pruning was applied at sparsity levels of 20%, 40%, and 60%. After pruning, models were fine-tuned where appropriate, and quantized versions were also generated for additional efficiency assessment.

D. Evaluation Metrics and Implementation

Models were evaluated using standard classification metrics: accuracy, precision, recall, F1-score, and area under the ROC curve (AUC). Efficiency was measured by model size (in MB), compression ratio relative to the dense baseline, and inference latency (in milliseconds). Quantized model sizes were recorded to estimate further deployment benefits. Security-relevant aspects were assessed through adversarial robustness using Fast Gradient Sign Method (FGSM) perturbations and interpretability via permutation feature importance. The strongest features consistently included number_offers, contract_value, log_contract_value, day_of_week, and year, aligning with domain knowledge on competition and pricing risks.

Experiments were implemented in Python using PyTorch for model training and pruning. The dataset was divided using a stratified train/test split of 80%/20% (427 training records, 107 test records), preserving the anomaly class distribution. A fixed random seed of 42 was applied throughout all experiments to ensure reproducibility. The enhanced MLP architecture comprised: Input (111 features) → Batch Normalization → Dense(256, ReLU) → Dropout(0.3) → Dense(128, ReLU) → Dropout(0.2) → Dense(64, ReLU) → Dense(1, Sigmoid), totalling approximately 50,000 parameters. Training used the Adam optimizer (learning rate = 1×10^{-3} , weight decay = 1×10^{-4}), binary cross-entropy loss, batch size of 32, up to 100 epochs with early stopping (patience = 15, monitored on validation AUC), and a 10% hold-out validation split drawn from the training set. Structured pruning used PyTorch’s `torch.nn.utils.prune.l1_structured` to remove entire neurons ranked by L1-norm; unstructured pruning used `torch.nn.utils.prune.l1_unstructured` with global magnitude thresholding. Because PyTorch’s default pruning API stores both the weight tensor and a binary mask, unstructured pruned models exhibit larger checkpoint sizes than the dense baseline; realizing actual memory savings requires conversion to a sparse representation using a compatible inference engine. Lottery Ticket pruning iterated three rounds of 20% magnitude pruning, resetting surviving weights to their initial values before fine-tuning for 30 epochs per round. FGSM adversarial perturbations were applied at $\epsilon = 0.1$ on normalized test features. All reported results are averaged over five independent runs with different random seeds.

II. RESULTS AND DISCUSSION

A. Results

We evaluated three pruning strategies — structured magnitude pruning, unstructured magnitude pruning, and Lottery Ticket-inspired pruning — using an enhanced MLP architecture on the weakly supervised TED procurement

dataset. The experiments were designed to answer the following research questions:

(1) Can model pruning maintain or improve predictive performance on weakly supervised procurement anomaly detection while substantially reducing model size and computational cost?

(2) How well do the pruned models improve practical edge-deployment proxies (memory footprint, inference latency, and quantized size) while retaining robustness under adversarial perturbations?

The dense baseline MLP model achieved an accuracy of 0.8131, F1-score of 0.8387, precision of 0.8387, recall of 0.8387, and AUC of 0.9002, with a model size of 0.0974 MB and an average inference latency of approximately 0.142 ms.

Table 1 summarizes the performance of the dense baseline and all pruned configurations at sparsity levels of 20%, 40%, and 60%

TABLE 1. COMPARISON OF DENSE BASELINE AND PRUNING STRATEGIES ON THE TED DATASET.

Strategy	Sparsity	AUC	F1-Score	CR	Size (MB)	Latency
Dense Baseline	0.0	0.9002	0.8387	1.00	0.0974	0.142
Structured Magnitude	0.2	0.9077	0.8387	1.33	0.0733	0.078
Structured Magnitude	0.4	0.9111	0.8320	1.91	0.0510	0.070
Structured Magnitude	0.6	0.8986	0.8226	3.03	0.0322	0.075
Unstructured Magnitude	0.2	0.9029	0.8387	0.51	0.1917	0.146
Unstructured Magnitude	0.4	0.8989	0.8387	0.51	0.1917	0.138
Unstructured Magnitude	0.6	0.9059	0.8640	0.51	0.1917	0.144
Lottery Ticket	0.2	0.8977	0.8460	0.64	0.1511	0.119
Lottery Ticket	0.4	0.9018	0.8480	0.86	0.1138	0.120
Lottery Ticket	0.6	0.9072	0.8571	1.27	0.0764	0.150

The best overall result was obtained with structured magnitude pruning at 40% sparsity, which slightly improved the AUC to 0.9111 while achieving a compression ratio of 1.91×, reducing the model size to 0.0510 MB, and lowering the inference latency to 0.070 ms. It should be noted that unstructured pruning configurations report model sizes larger than the dense baseline (0.1917 MB vs. 0.0974 MB) and compression ratios below 1.0. This is because PyTorch’s default pruning API retains both the original weight tensor and a binary mask in the checkpoint, effectively doubling storage. Realizing actual memory savings from unstructured pruning requires converting the masked model to a sparse format (e.g., CSR or COO) using a sparse-aware inference engine. The quantized model sizes reported in Table 1

reflect post-conversion estimates and represent the practically achievable footprint.

Figs. 1–6 illustrate the detailed trade-offs between sparsity level and individual performance metrics for the three pruning strategies.

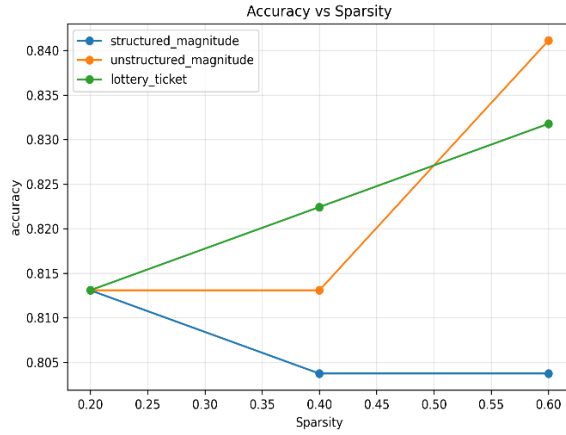


Fig. 1. Accuracy versus sparsity level for the three pruning strategies.

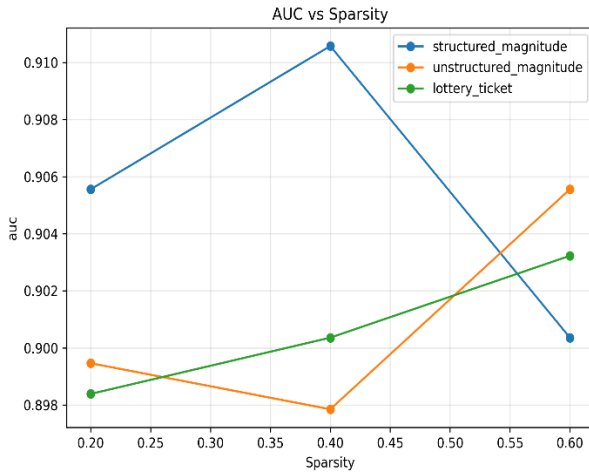


Fig. 2. AUC versus sparsity level for the three pruning strategies.

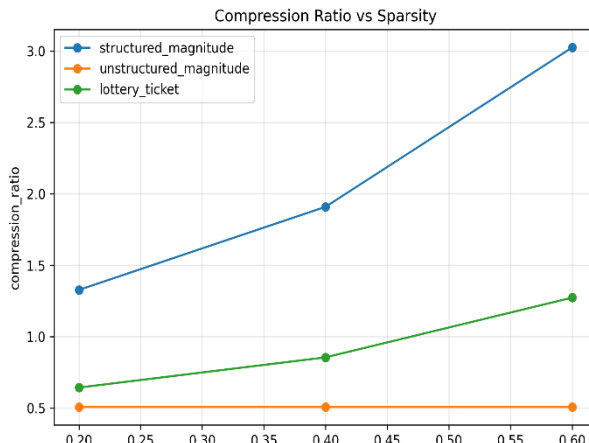


Fig. 3. Compression ratio versus sparsity level for the three pruning strategies.

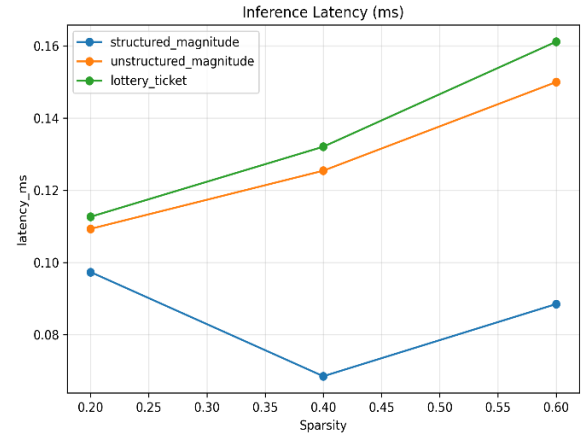


Fig. 1 Inference latency versus sparsity level for the three pruning strategies.

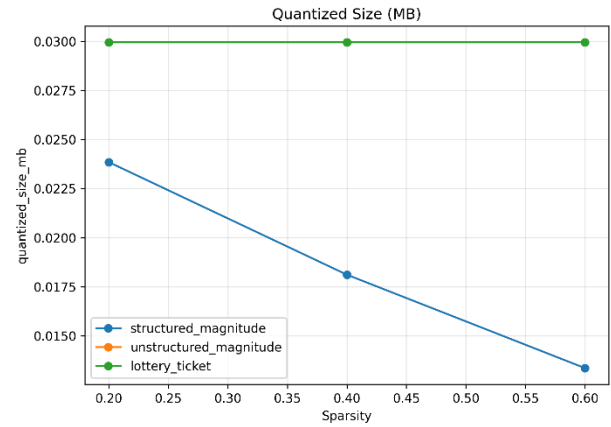


Fig. 2 Quantized model size versus sparsity level for the three pruning strategies.

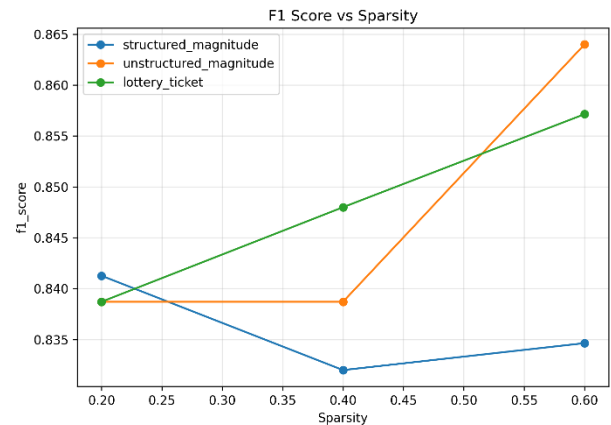


Fig. 3 F1-score versus sparsity level for the three pruning strategies.

B. Answering the Research Questions

Regarding the first research question, the results confirm that model pruning can maintain and even slightly improve predictive performance while substantially reducing model complexity. Structured magnitude pruning

at 40% sparsity achieved a higher AUC (0.9111) than the dense baseline (0.9002) with a $1.91\times$ compression ratio. This demonstrates that effective pruning successfully removes redundant parameters without sacrificing the model's ability to detect key corruption signals such as single-bid awards and irregular pricing patterns. For the second research question, the pruned models showed clear improvements in practical edge-deployment proxies. Structured magnitude pruning significantly reduced inference latency (from 0.142 ms to 0.070 ms) and memory footprint. Quantized model sizes were also substantially smaller, particularly with the structured pruning approach. However, adversarial robustness remained moderate, with AUC dropping to approximately 0.8052 under FGSM perturbations, indicating that additional robustness techniques may be required for high-security applications.

C. Discussion

The experimental results demonstrate that model pruning, particularly structured magnitude pruning, represents an effective approach for developing lightweight yet accurate procurement anomaly detection models. The demonstrated capacity to reduce model size and inference latency while maintaining or improving AUC supports deployment in real-world settings, including edge devices used in military and public-sector monitoring systems. From a security perspective, these compact models support near-real-time detection of procurement risk signals — such as single-bid awards, abnormally short tender windows, and irregular fund flows — in defense logistics and governance frameworks. The reduced computational footprint also lowers the attack surface in secure environments and decreases energy consumption. Compared to prior studies that primarily emphasize predictive accuracy on large-scale models [7], [8], this work advances the field by combining real TED procurement data with systematic pruning and security-focused evaluation metrics. While some related works report higher absolute accuracy, they rarely address the critical constraints of edge deployment and adversarial robustness in security-critical applications.

Nevertheless, the moderate drop in performance under adversarial perturbations highlights the need for complementary techniques such as adversarial training. Overall, this study provides a promising pathway for integrating efficient, trustworthy AI into secure systems for enhanced societal integrity and resilience in public procurement and defense sectors

III. CONCLUSIONS

This study investigated the effectiveness of model pruning techniques for developing lightweight procurement anomaly detection models suitable for deployment in secure and resource-constrained environments. Using the TED dataset focused on

Bulgarian public tenders in 2023, a baseline enhanced MLP was trained and compared against three pruning strategies. The experiments show that at 40% sparsity, structured magnitude pruning provided a good trade-off between predictive accuracy and model efficiency. It achieved an AUC of 0.9111 (vs 0.9002 for the dense baseline), while delivering a compression ratio of 1.91, reducing model size to 0.0510 MB, and decreasing inference time to 0.070 ms. This configuration is well suited for edge deployment in defense logistics, public sector monitoring, and infrastructure protection. Experiments demonstrated that model pruning can effectively reduce the key deployment barriers facing AI-based procurement risk monitoring systems — namely high computational and memory requirements and limited suitability for resource-constrained environments — while incurring only modest performance reductions with respect to key procurement risk signals such as single-bid awards, abnormally short tender windows, and price anomalies. Although the models showed moderate sensitivity to adversarial perturbations, the permutation importance analysis enhanced trustworthiness by identifying features aligned with established domain expertise in procurement risk assessment.

In conclusion, this work demonstrates that compact, efficient, and reasonably robust procurement anomaly detection models can be successfully developed through pruning techniques, contributing toward the broader goal of trustworthy AI for governance monitoring. The significant reduction in model size and latency opens promising opportunities for implementation on embedded and resource-limited hardware in real-world security-related applications. These results should be interpreted as a proof-of-concept demonstration, given the weakly supervised labeling setup and the single-country, single-year dataset scope; further validation on larger, multi-country datasets and confirmed ground-truth labels is required before operational deployment.

Future work will focus on expanding the dataset with multi-country TED records, combining pruning with adversarial training and quantization techniques to further enhance robustness and efficiency, and conducting practical deployment tests on tiny embedded devices and edge hardware. Integrating these lightweight models into operational decision support systems will be crucial for strengthening societal resilience against corruption in governance and defense sectors.

IV. ACKNOWLEDGMENTS

The present paper was prepared as a result of the scientific research activities conducted within scientific project “Research on the possibilities of preventing corruption activities” financed by the Bulgarian National Science Fund at the Ministry of Education and Science, “Competition for financial support of basic research projects – 2025”, Contract № KII-06-H95/7 by 09.12.2025

REFERENCES

- [1] Transparency International Defence & Security, "Governance First: Tackling Corruption Risks Amid Rising Defence Spending," Transparency International Defence & Security, Apr. 2026. [Online]. Available: <https://ti-defence.org/publications/governance-first-tackling-corruption-risks-amid-rising-defence-spending/>
- [2] Transparency International US and Transparency International Defence & Security, "Blissfully Blind: The New US Push for Defense Industrial Collaboration with Partner Countries and its Corruption Risks," Transparency International, Apr. 2024. [Online]. Available: <https://us.transparency.org/app/uploads/2024/04/Blissfully-Blind-US-Push-for-Defense-Industrial-Collaboration-WEB-New-1.pdf>
- [3] Transparency International Defence & Security, "Trojan Horse Tactics: Corruption Risk in Defence Spending," Transparency International Defence & Security, 2024. [Online]. Available: <https://ti-defence.org/wp-content/uploads/2024/04/Trojan-Horse-Tactics-corruption-risk-in-defence-spending.pdf>
- [4] Transparency International, "Corruption Perceptions Index 2025," Transparency International, Feb. 2026. [Online]. Available: <https://www.transparency.org/en/cpi/2025>
- [5] M. Resimić, "Harnessing artificial intelligence (AI) for anti-corruption," Transparency International Knowledge Hub, Oct. 2025. [Online]. Available: https://knowledgehub.transparencycdn.org/kproducts/Harnessing-artificial-intelligence-for-anti-corruption_01.10.2025.pdf
- [6] T. Zatonatska, O. Dluhopolskyi, O. Artiushenko, I. C. Lopes, A. Ignatyuk, and O. Liubkina, "Comparative analysis of ensemble machine learning models for risk-oriented monitoring of military procurement," *Journal of Risk and Financial Management*, vol. 19, no. 3, p. 170, 2026, doi: <https://doi.org/10.3390/jrfm19030170>.
- [7] C. Cernăzanu-Glăvan and A.-Ş. Bulzan, "Explainable AI and fuzzy linguistic interpretation for enhanced transparency in public procurement: Analyzing EU tender awards," *Mathematics*, vol. 13, no. 13, p. 2215, 2025, doi: <https://doi.org/10.3390/math13132215>.
- [8] OECD (2025), *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, OECD Publishing, Paris, <https://doi.org/10.1787/795de142-en>.
- [9] G. Piras, M. Pintor, A. Demontis, B. Biggio, G. Giacinto, and F. Roli, "Adversarial pruning: A survey and benchmark of pruning methods for adversarial robustness," *Pattern Recognition*, vol. 168, p. 111788, 2025, doi: <https://doi.org/10.1016/j.patcog.2025.111788>.
- [10] A. Douzandeh Zenoozi, L. Erhan, A. Liotta, and L. Cavallaro, "A comparative study of neural network pruning strategies for industrial applications," *Frontiers in Computer Science*, vol. 7, p. 1563942, 2025, doi: <https://doi.org/10.3389/fcomp.2025.1563942>.
- [11] J. Frankle and M. Carbin, "The lottery ticket hypothesis: Finding sparse, trainable neural networks," *arXiv preprint arXiv:1803.03635*, 2018.
- [12] P. Austria *et al.*, "The effects of compounded reductions on adversarial robustness (pruning and robustness)," *OSTI*, 2025. Available: <https://www.osti.gov/servlets/purl/3002675>.
- [13] E. Schneider dos Santos, M. Machado dos Santos, M. Castro *et al.*, "Detection of fraud in public procurement using data-driven methods: a systematic mapping study," *EPJ Data Science*, vol. 14, p. 52, 2025, doi: <https://doi.org/10.1140/epjds/s13688-025-00569-3>
- [14] L. Potin, R. Figueiredo, V. Labatut, and C. Langeron, "Pattern mining for anomaly detection in graphs: Application to fraud in public procurement," in *Machine Learning and Knowledge Discovery in Databases: Applied Data Science and Demo Track (ECML PKDD 2023)*, G. D. F. Morales *et al.*, Eds. Lecture Notes in Computer Science, vol. 14174. Cham, Switzerland: Springer, 2023, pp. 1–? doi: https://doi.org/10.1007/978-3-031-43427-3_5.
- [15] U. U. Acikalin, M. K. Gorgun, M. Kutlu, and B. K. O. Tas, "How you describe procurement calls matters: Predicting outcome of public procurement using call descriptions," *Natural Language Engineering*, vol. 30, no. 6, pp. 1255–1276, 2024. doi:<https://doi.org/10.1017/S135132492300030X>
- [16] B. Liu *et al.*, "A Survey of Lottery Ticket Hypothesis," *arXiv preprint arXiv:2403.04861*, 2024. [Online]. Available: <https://arxiv.org/pdf/2403.04861>
- [17] R. Bluteau, R. Gras, and G. Peralta, "Genetic-based lottery ticket pruning for transformers in sentiment classification: Realized through lottery sample selection," *Algorithms*, vol. 18, no. 12, p. 798, 2025, doi: <https://doi.org/10.3390/a18120798>.
- [18] OECD, *Digital Transformation of Public Procurement*, OECD Publishing, Paris, 2025. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/digital-transformation-of-public-procurement_90ace30d/79651651-en.pdf.
- [19] OECD, "AI in fighting corruption and promoting public integrity," in *Governing with Artificial Intelligence*, OECD Publishing, Sep. 2025. [Online]. Available: https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/ai-in-fighting-corruption-and-promoting-public-integrity_60f5c50a.html
- [20] Transparency International Defence & Security, "The Trust Gap: How Public Trust Links to Defence Spending," Transparency International Defence & Security, Mar. 2026. [Online]. Available: <https://ti-defence.org/the-trust-gap-how-public-trust-links-to-defence-spending/>

Environmental Security and Marine Ecosystem Protection: Addressing Regulatory Ambiguities in Bulgaria

Miroslava Robinson

dept. Ecology and Environmental Protection
Technical University of Varna
Varna, Bulgaria
miroslava.robinson@tu-varna.bg

Daniela Toneva

dept. Ecology and Environmental Protection
Technical University of Varna
Varna, Bulgaria
dtoneva@abv.bg

This report focuses on mechanisms to ensure environmental security and in particular protection of the marine environment from pollution, including the impact from incidents, disasters, accidents and other emergency situations. The presented analysis at the complex of measures and activities implemented in Bulgaria for prevention and response to pollution of the marine environment which reveals a number of gaps both in regulatory and organizational aspects. It has been demonstrated that an objective necessity to expanded the scope of mechanisms for ensuring environmental security in coastal waters, territorial sea and exclusive economic zone of the Republic of Bulgaria. Suggestions for the development of the environmental security system are proposed which would ensure regulatory compliance as well as real improvement in the effectiveness for the protection of the Black Sea against pollution.

Keywords— *Black Sea, environmental security, marine environment, risk management.*

I. INTRODUCTION

Environmental security has become a defining concept in contemporary governance responding to recognition of environmental degradation as a threat to human wealth, economic stability and geopolitical order. It takes into account the change in the traditional concept of security to a multispectral frame of environmental risks – pollution, climate change, biodiversity loss [1], [2], [3].

The specific and unique characteristics of the Black Sea - limited water exchange, fresh water balance, stratified layers and dependence from river flow presents high ecological sensitivity as well as significantly reduce capacity to recover after environmental disturbances. Consequently, even a moderate anthropogenic pressure – incident can result in a long term and irreversible environmental impact [4].

The Black sea is a critical marine transport corridor linking Europe, Asia and middle East, also a semi-closed basin with limited water exchange, unique structure of anoxic layers, vulnerable to pollution, environmental disturbances and anthropogenic pressure - industrial discharge, agricultural runoff, marine transport.

In the Bulgarian context environmental security is complicated by regulatory fragmentation and institutional overlap. As a coastal state and European Union member it operates within a comprehensive legal framework of European directives and international agreements but the effectiveness of these mechanisms remains constrained by coordination deficits and implementation gaps.

The increasing complexity of environmental risks in the Black Sea region – particularly associated with military activities requires more adaptive and integrated governance approach.

II. MATERIALS AND METHODS

The regulatory requirements for practices and control are reviewed taking into account international activities, national legislation and normative documents concerning the protection of marine environment in its entirety. The analysis is focused on identifying gaps and ambiguities or inconsistency in the regulation of minimum requirements in order to achieve and maintain Good Environmental Status of the Black Sea ecosystem and in this aspect of Bulgarian environmental security.

A comparison between the regulatory requirements and the practice in the field of marine environmental protection was made as an element of ecological security. A review of public available data and risk for ecological security has been conducted in particular for the Bulgarian part of Black Sea based on the conceptual method DPSIR (Driver-Pressure-State-Impact-Response).

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.151>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

III. RESULTS AND DISCUSSION

Environmental security is a fundamentally multidisciplinary concept that integrates ecological sustainability with political and socioeconomic stability. It is defined as the protection of the ecosystems and human society from environmental risks arising from natural and anthropogenic activities. Modern interpretations connect the interdependence between environmental degradation and security threats, highlighting how the ecological stress could trigger economic decline, migration and conflict [5], [6]. The key elements of environmental security are presented in Table 1.

TABLE 1 KEY ELEMENTS TO ENVIRONMENTAL SECURITY

Element	Key element characteristics	
	Description	Condition
Environmental quality	The state of air, water, soil and overall environmental components	Clean, safe, stable and productive according to the requirements and standards
Environmental functions	The ability to provide ecosystem services	Support life and human activities
Environmental risk	Threats as pollution, climate change, resource depletion, extreme weather condition and natural disasters	Risks are defined or predicted, minimized and manageable

The Black Sea region presents a particular and a complex case of environmental security. It is a semi-closed basin connected to Mediterranean Sea through Bosphorus Strait and the Sea of Azov through the Kerch Strait. The system of currents is under the influence of the largest European rivers flowing into the northern west part of the basin – Danube, Dnieper and Dniester [7]. The fresh water from rivers, atmospheric precipitation and the inflow of saline mediterranean waters create a specific thermohaline profile of the Black Sea. Strong and stable vertical stratification and anoxic layer with high hydrogen sulfide concentration at depths below 150 m distinguish the basin from the World Ocean [4]. The physical characteristics and geographical position of the basin amplify environmental risk and require the implementation of complex measures for prevention and response to pollution of the marine environment in the event of incidents, disasters, accidents and other emergencies [4], [6], [7], [8]. The main type of threats to the Black Sea ecosystem are presented in Table 2.

TABLE 2 THREATS TO ECOSYSTEM

Type	Main threats to the ecosystem		
	Source	Pressure	Impact
Euthrophication	Agriculture, urban discharge	High	Oxygen depletion, biodiversity loss
Chemical pollution	Industry, marine transport	High	Toxicity and contamination

Type	Main threats to the ecosystem		
	Source	Pressure	Impact
Military activities	Conflict zones	High	Longterm ecosystem damage
Oil pollution	Marine transport, offshore drilling	High	Habitat pollution, biodiversity loss
Marine litter	Terrastrial sources, coastal activities, fishery and aquaculture, shipping	High	Ecosystem disruption, biodiversity loss
Invasive species	Ballast water	Medium	Food chain imbalance
Sound pollution	Marine transport, offshore drilling, military operations	Medium	Habitat disruption, change in the migration routes

The Black Sea ecosystem has experienced significant degradation over the recent decades due to cumulative anthropogenic pressures [4]. The presence of anoxic deep waters limits biological activity to the surface layers, rivers transport nutrients, pollutants and litter from vast inland areas. Land based pollution remains one of the most significant threats. Agricultural runoff, industrial discharge and wastewaters from urban areas contribute to eutrophication and chemical contamination.

The environmental protection system for marine environment in Bulgaria is formed in accordance to international legal framework, EU directives and regional documents presented in Table 3, 4 and 5. That includes Convention of prevention of Marine Pollution by Dumping Wastes and other matter (London Convention), International Convention for Prevention of Pollution from Ships (MARPOL 73/78), United Nation Convention on the Law of Sea (UNCLOS), International Convention on Oil Pollution Preparedness Response and Cooperation (OPRC), International Convention for the Control and management of Ships' Ballast water and Sediments (Ballast water convention).

TABLE 3 INTERNATIONAL DOCUMENTS FOR PROTECTION OF MARINE ENVIRONMENT

Document	Black Sea International documents	
	Description	Year
London Convention	Control of marine dumping	1972
MARPOL Convention	Ship pollution control	1973/78
UNCLOS	Law of the sea framework	1982
OPRC	Oil pollution emergency preparedness and response	1990
Ballast convention	Prevention of invasive species transfer via ballast waters	2004

OPRC, 1990 complements the preventive nature of MARPOL/73/78 and focuses on incident response. While

MARPOL aims to reduce the probability of pollution and limit routine and emergency discharges, OPRC establishes framework for preparedness and international cooperation in case of major oil spills. OPRC requires states to develop a national action plan as well as regional plans for Varna and Burgas, to provide equipment and personnel, common assistance at transboundary incidents.

A system with different levels is applied in Bulgaria with responsibilities divided between environmental, maritime, emergency, fishery and aquaculture control authorities characterized by a fragmented institutional structure. Responsibility is divided among Ministry of Environment and Water (MOEW) and Executive Agency maritime Administration (EAMA), Black Sea Basin Directorate (BSBD) and General Directorate Fire Safety and Civil Protection. MOEW is responsible for marine environmental policy regarding international, EU and regional documents - implementation of UNCLOS obligation on environmental protection, Marine Strategy Framework Directive (MSFD, 2008/56/EC), Water framework Directive (WFD, 2000/60/EC), London convention [9], [10], [11]. Through national legislation as Water Act, Environmental Protection Act, Biodiversity Protection Act and regional representatives as BSBD, EEA the ministry regulates activities in the sea, carries monitoring, data reporting at EC, pollution control and permitting regimes. EAMA at the Ministry of Transport is the main authority for MARPOL and the Ballast Convention. It is responsible for port state inspections and pollution standards, ballast water systems, certification of vessels. Executive Agency for Fisheries and Aquaculture (EAFV) as an administrative unit at ministry of Agriculture carries control of fishing activities and aquaculture ensuring sustainable development.

All this division reflects the management of marine environment combines environmental protection, maritime transport regulation and emergency response and also creates significant coordination challenges. One of the main difficulties is overlap of competencies – protection of the marine environment and quality of marine waters under MOEW and its regional representative BSBD, while pollution from the ships is regulated by EAMA and fishery by EAFV.

TABLE 4 EU DOCUMENTS FOR PROTECTION OF MARINE ENVIRONMENT

Document	EU Directives	
	Description	Year
Bird Directive, 2009/147/EC	Coastal ecosystems	1979
Habitats Directive 92/43/EEC	Marine NATURA 2000 areas	1992
Water Framework Directive, 2000/60/EC	Water quality in coastal waters, GES	2000
Marine Strategy Framework Directive, 2008/56/EC	Marine environment GES	2008
Maritime Spatial Planning Directive, 2014/89/EU	Spatial governance in marine environment	2014

In practice many of the marine pollution issues - oil spills, ballast water discharge requires joint action. The absence of clearly dominating and coordinating authority leads to delays and unclear accountability, institutional fragmentation weakens timely monitoring and control mechanisms. Although EEA collects monitoring data on marine environment ordered by BSBD and EAMA conducts ship inspections there is not a mechanism for an exchange of information which creates a gap in detection of pollution especially in cases of illegal discharges or non-compliance by vessels.

EU addresses marine environment most notably through MSFD [9] and WFD [10] MSFD establishes a comprehensive approach to protection of marine waters requiring from Member States to achieve „Good environmental Status“ (GES) via ecosystem based management, monitoring programmes and policy measures, transborder coordination in the same regions such as Black Sea. Water Framework Directive (WFD, 2000/60/EC) provides water management on river basin principle, assessment of the quality, recognising that inland and coastal waters are connected. WFD also establishes prevention of water deterioration, water biodiversity and pollution control at the source.

Black Sea region is also addressed by EU strategic approach which is based on three pillars – security and stability, economic development, environmental protection and resilience. The environmental pillar emphasizes on the importance of climate adaptation, pollution control and ecosystem restoration with focus on environmental sustainability. The effectiveness of this current strategy is limited by funding, technological capacity and coordination at regional level.

TABLE 5 REGIONAL DOCUMENTS FOR PROTECTION OF MARINE ENVIRONMENT

Document	Black Sea regional documents	
	Description	Year
Bucharest Convention	Regional framework at basin level	1992
Black Sea Biodiversity Protocol	Biodiversity conservation	2002
Black Sea Strategic Plan	Pollution reduction	2007
Black Sea Monitoring and Assessment Plan	Initial monitoring for the basin	2009

Bucharest Convention at the Black Sea level sets the main guidelines for prevention, reduction and control of marine pollution, conservation of biodiversity, restoration of ecosystem services [12]. Convention and associated protocols provide cooperation among Black Sea countries and advisory groups have been established to provide coordinated regional action. Advisory groups participation and reporting in Bulgaria is divided between several organizations – BSBD (MOEW), EAMA (MT), Institute of Oceanology – Bulgarian Academy of Science, Ministry of Regional Development and Public works.

Environmental security does not have a definition in the Bulgarian legal framework. National regulation includes EU directives transposed into Bulgarian presented in Table 6.

TABLE 6 NATIONAL REGULATIONS FOR PROTECTION OF MARINE ENVIRONMENT

Document	National regulations	
	Description	Year
Environmental Protection Act	Environmental protection	2002
Water Act	Protection of water resources on basin principle	1999
Maritime Spaces, Inland Waterways and ports of Republic of Bulgaria Act	Regulates Bulgarian maritime zones, inland waters, navigation and ports.	2000
Biodiversity Act	Protection of biodiversity	2002
Black Sea Spatial Planning Act	Framework for maritime spatial planning	2021
Environmental Liability Act	Ecological responsibility, „the pollutant pay“ principle	2008

Despite all legal framework significant challenges remain in Bulgaria regarding environmental security. The main critical is fragmentation of governance – responsibilities for environmental protection, maritime policy and emergency response are distributed across different institutions. Duplicating the functions delays decision making and leads to inefficiency in case of incidents, disasters, accidents and other emergency situations. Also the lack of use of modern technologies proven for remote monitoring – drones or access to satellite images not used. The advantages of drone technology – high mobility, ability to reach dangerous and restricted locations, reduction of risk in emergency situation, time and cost effective as well as improved coordination between different institution involved make them a key element of environmental security [13], [14].

The environmental protection of Black Sea region is a complicated and challenging process with regulatory fragmentation especially in the current geopolitical situation. Military activities on the territory of Ukraine introduced new risks including oil spills from damaged infrastructure and vessels, chemical contamination, noise pollution and marine litter. These threats need to be adequately addressed by current legal frame [15]. Environmental security in the Black Sea requires an integrated governance approach combining legal harmonisation, institutional coordination and regional cooperation [16], [17].

First key element needed for development of environmental security in Bulgaria is legal harmonization to ensure consistency of national law international agreements. Second key is strengthening national coordination, improved communication and collaboration of competent authorities. Third key is monitoring and modern technology – drones, satellites to support decision

making at incidents, disasters, accidents and other emergency situations.

IV. CONCLUSIONS

Environmental security and marine ecosystem protection in Bulgaria represents a complex and evolving challenge formed by vulnerability, geopolitical instability, regulatory fragmentation and overlapping responsibility. Although an international and EU comprehensive legal framework is established, significant gaps remain in the implementation and coordination at national level. A need has been revealed for the key requirements to go beyond the existing regulation to achieve real environmental security. Addressing these challenges requires an integrated governance approach that combines legal harmonization, institutional coordination and technology implementation. A comprehensive system on environmental security in Bulgaria needs to focus on several key elements -harmonization of law, institutional coordination, accountability and investment in modern technology for distance monitoring and observation. Strengthening the environmental security system of Bulgaria will contribute to stability and sustainability of the Black Sea region.

REFERENCES

- [1] G. Zurlini, and F. Müller, Felix. Environmental Security, 2008. <https://doi.org/10.1016/B978-008045405-4.00707-2> [Accessed March 25, 2026]
- [2] J. Tian, J. and G. Gang, "Research on regional ecological security assessment", Energy Procedia, vol., part B,16, pp.1180-1186, 2012.
- [3] Gilek, M., Kern, K. Governing Europe's Marine Environment: Europeanization of Regional Seas Or Regionalization of EU Policies? Routledge, 2016. [E-book]. ISBN 9781315585543.
- [4] United Nations Environmental Programme, Black Sea Pollution Assessment. United Nations Publication Sales No.E.99.III.R.2, Volume 10, Black Sea Environmental Series. 1998. ISBN 92-1-129506-8
- [5] Liu, C., Li, W., Xu, J., Zhou, H., Li, C., & Wang, W. „Global trends and characteristics of ecological security research in the early 21st century: A literature review and bibliometric analysis“, Ecological Indicators, vol.137, April 2022, 108734. <https://doi.org/10.1016/j.ecolind.2022.108734>
- [6] Kvach, Y., Stepien, C. A., Minicheva, G. G., & Tkachenko, P., „Biodiversity effects of the Russia–Ukraine War and the Kakhovka Dam destruction: ecological consequences and predictions for marine, estuarine, and freshwater communities in the northern Black Sea. Ecological Processes, 14(1), pp. 1-25, Dec 2025. <https://doi.org/10.1186/s13717-025-00577-1>
- [7] R. Toderascu & E. Rusu, „Evaluation of the Circulation Patterns in the Black Sea Using Remotely Sensed and in Situ Measurements“, International Journal of Geosciences, vol.4, pp.1009-1017, 2013. <http://dx.doi.org/10.4236/ijg.2013.47094>
- [8] A. Atanasov, „Black sea facing an ecological disaster the legal framework for protection of marine biodiversity“, Journal of Global resources, vol.5, pp.15-19, 2017. ISSN 2455-2445.
- [9] European Commission, „Directive 2008/56/EC of the European parliament and of the council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive)“, Off. J. Eur. Union L–21 (L 164/ 1, 25.6.2008).
- [10] Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy , The official

- publication is in the Official Journal of the European Communities L327, 22/12/2000, pp. 1-73.
- [11] Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Matter, 1972. [Online] Available: <https://www.imo.org/en/ourwork/environment/pages/london-convention-protocol.aspx> [Accessed March 22, 2026].
- [12] M. Aydın, „Regional cooperation in the Black Sea and the role of institutions", *Perceptions: Journal of International Affairs*, vol.10(3), pp. 57-83. 1 September, 2005. Available: <https://dergipark.org.tr/en/pub/perception/article/625150>
- [13] A. Atanasov & A. Bankova, „The influence of location accuracy on the estimation of crops with a budget UAV in Dobrudja region", *Bulgarian Journal of Agricultural Science*, vol.29 (1), pp. 176-181, Available: <https://www.agrojournal.org/29/01-21.pdf>
- [14] V. Bhandari, "Use of Technology in Disaster Management", *Unity Journal*, vol. 3(1), pp. 292-304, 6 March, 2022. <https://doi.org/10.3126/unityj.v3i01.43333>.
- [15] N. Oral, „The legal framework of cooperation for protection of marine biodiversity in the Black Sea", *Revue juridique de l'Environnement*, vol. 37(2), pp. 255-267, 2012. Available: https://droit.cairn.info/article/RJE_122_0255
- [16] A.M .Hasan, „Environmental and Transboundary Impacts of Naval Mine Warfare in the Black Sea: Legal and Ecological Perspectives", *Journal of Anatolian Environmental and Animal Sciences*, March 30, 2026. <https://doi.org/10.35229/jaes.1894561>
- [17] N. Algan, & , G. K. Aydoğan, „Russian Federation- Ukraine war as an environmental security issue on the Black Sea", *Journal of the Black Sea/Mediterranean Environment*, vol. 29(1), pp. 49-72, 2023. <http://doi.org/10.18352/ulr.409>

Application of the Broken Windows Theory in the Context of Military Organizational Behavior and Discipline

Sabin Sabev

Branch in Veliko Tarnovo
University of Agribusiness
and Rural Development
Plovdiv, Bulgaria
ssabev@uad.bg

Abstract — This article examines the applicability of the criminological broken windows theory in the context of military organizational behavior and the maintenance of military discipline. The conceptual link between this theory and the phenomenon of normalization of deviance is analyzed, and their mutual complementarity in explaining the processes of disciplinary erosion within military organizations is substantiated. The study is of a theoretical-analytical character and traces the mechanisms through which the toleration of seemingly minor violations gradually weakens the organizational culture and creates the preconditions for more serious deviations.

Keywords — broken windows theory, military discipline, organizational culture, normalization of deviance

I. INTRODUCTION

Military discipline is the foundation upon which combat readiness, unit cohesion, and ultimately the ability of the armed forces to fulfill their constitutional tasks are built. The maintenance of discipline is simultaneously a legal obligation, a managerial function, and a cultural phenomenon that is not exhausted by the formal observance of normative prescriptions.

The broken windows theory is a criminological concept formulated by James Q. Wilson and George L. Kelling in an article published in *The Atlantic Monthly* in 1982 [1]. It offers an explanation of the processes through which visible disorder and the toleration of minor violations create an environment conducive to escalation toward more serious antisocial manifestations. Although developed in the context of urban crime and policing, the theory possesses considerable analytical potential for other structured hierarchical environments, such as military organizations.

According to the authors, the visible signs of disorder and antisocial behavior in the urban environment create conditions that encourage further disorder and crime, including more serious forms of offenses. This theoretical proposition is also supported by an earlier experiment conducted by another researcher, in which an abandoned automobile in a neighborhood with visible signs of disorder was rapidly vandalized and destroyed, while an identical automobile in a well-maintained environment remained untouched for a longer period.

The application of the theory in the context of the armed forces may yield specific and measurable practical benefits. On the one hand, it provides the command staff with an instrument for the early identification and counteraction of persistent negative group habits that traditionally undermine military discipline: non-regulation interpersonal relations between service members, the systematic toleration of tardiness and lapses in duty assignments, a formalistic attitude toward the maintenance of equipment and weaponry, and the selective observance of requirements concerning appearance and military courtesy. On the other hand, the consistent application of the principle of repairing the broken windows contributes to the strengthening of trust along the chain of command, to the enhancement of combat readiness through a daily maintained standard, and to the formation of a sustainable organizational culture in which the written rules correspond to actual conduct.

On this basis the working hypothesis of the present study is formulated: the consistent counteraction of seemingly minor violations within the military organization, by analogy with the repairing of broken windows, leads to a sustained improvement of the disciplinary environment, the limitation of negative group habits, and the reduction of the preconditions for serious organizational failures.

II. MATERIALS AND METHODS

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.54>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

The present study is of a theoretical-analytical and interdisciplinary character. It is not based on empirical data collected specifically for its purposes, but on the analysis and juxtaposition of established scientific concepts with the current normative framework.

The materials employed may be grouped into three categories. The first encompasses classical scientific works in the fields of criminology, the sociology of organizations, and safety science: the original exposition of the broken windows theory by Wilson and Kelling [1] and its extended practical elaboration by Kelling and Coles [13]; Harcourt's critical analysis of the empirical foundations of the theory [2]; Diane Vaughan's study of the Challenger Space Shuttle disaster and the normalization of deviance [3]; the works of James Reason on the management of organizational risks and safety culture [10]; the research of Weick and Sutcliffe on high-reliability organizations [11]; Sidney Dekker's conception of a just culture [12]; and Goffman's analytical framework concerning total institutions [8]. The second category encompasses the current normative framework of the Republic of Bulgaria in the field of defense and the armed forces: the Law on Defense and the Armed Forces [4]; the Regulations on Military Service of 2025 [5]; the previous Regulations on Military Service of 2008, used for comparative purposes [6]; and the Implementing Regulations of the Law on Defense and the Armed Forces [7]. The third category comprises theories explaining the behavioral mechanisms within the organization — above all, Bandura's social learning theory [9].

The following scientific methods have been applied in the study: the deductive-analytical method, the comparative method, conceptual analysis, normative-legal analysis, and the combined methods of synthesis and induction. The deductive-analytical method permits the derivation of specific consequences for the military organization from general theoretical premises. The comparative method has been applied in the juxtaposition of the criminological context in which the theory was originally formulated with the military organization as a particular type of institutional environment. Conceptual analysis is directed toward tracing the connection and interaction between the broken windows theory and the concept of normalization of deviance, as well as toward their synthesis within a common explanatory framework. Normative-legal analysis has been applied to the interpretation of the relevant provisions of the Law on Defense and the Armed Forces and of the Regulations on Military Service in the light of the theories under consideration. Finally, through the methods of synthesis and induction, a model for the prevention of disciplinary erosion applicable to the conditions of the armed forces has been derived.

III. EXPOSITION

The fundamental postulates of the broken windows theory may be synthesized as follows: visible disorder — graffiti, broken windows, litter, damaged infrastructure — signals to potential offenders that social control in a given environment has weakened. Furthermore, the environment communicates with its participants: a single broken window that remains unrepaired conveys the message that society is unable or unwilling to defend itself against violations. The result is a weakening of informal social control and a reinforcement of the perception that the rules are conditional. In this sense, disorder is not merely a backdrop, but an active signaling mechanism.

In this regard, the theory rests upon three interrelated elements of social control: norms defining expectations for behavior; monitoring — the observation of compliance with the norms; and signaling through the visual and behavioral indicators of what the actual, rather than the formally declared, state of affairs is.

The broken windows theory has found its most extensive application in the context of policing. Kelling and Coles developed and systematized the practical aspects of its implementation in an extensive study devoted to the restoration of order and the reduction of crime in the urban environment [13]. The most well-known practical implementation of the theory took place in New York under the leadership of Police Commissioner William Bratton (1994–1996), whose Quality-of-Life initiative was directed against minor offenses — fare evasion in the subway, public drinking, panhandling, and disorder. By 1996, when Bratton left his post, serious crimes in New York had decreased considerably and the number of homicides had fallen by approximately half. These data, however, should not be read as unequivocal proof that the effect was attributable solely to the application of the theory.

At the same time, the theory has been the subject of serious scholarly criticism. It has been pointed out that its aggressive application may lead to over-repression against marginalized communities, that alternative explanations exist for the decline in crime — demographic changes, economic factors, changes in police statistics — and that the causal link between disorder and serious crime has not been fully demonstrated empirically [2]. Consequently, the theory may be employed primarily as an explanatory and cautionary framework rather than as a universal causal law. Despite the criticisms directed at it, the theory remains highly influential and has been transposed beyond criminology — into education, healthcare, and organizational management.

The broken windows theory is convincingly complemented by the concept of normalization of deviance. This concept was formulated by Diane Vaughan, a sociologist at Columbia University, in her study *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (1996), devoted to the disaster of the Space Shuttle Challenger on 28 January 1986 [3].

Vaughan defines the normalization of deviance as a gradual process in which persons within an organization become so accustomed to a particular deviation from the rules that they cease to perceive it as a deviation, even though it clearly exceeds their own safety standards. The key mechanism is accumulation: a one-time deviation may arise under external pressure, but if it does not lead to immediate adverse consequences it establishes a precedent for future tolerance. Over time, repetition displaces the official perception of normalcy.

In the case of the Challenger, engineers had repeatedly observed erosion of the O-rings during previous flights, but since none of these observations had resulted in a catastrophe, the deviation gradually came to be perceived as acceptable. Instead of being treated as a warning signal, the recurring damage to the seals became an expected and tolerated element of operations. With each successive successful flight, the threshold of acceptable risk shifted upward and the sense of danger diminished. On 28 January 1986, during a launch in unusually low temperatures, the O-rings ultimately failed, leading to the

destruction of the shuttle and the death of its seven crew members. The tragedy demonstrates that the true danger lies not solely in a single technical defect, but in the institutional culture that gradually erases the boundary between the permissible and the fatal.

In a similar manner, within military organizations, when the circumvention of the rules becomes routine and routine violations are perceived as customary practice, the average service member adopts them as the *de facto* standard of behavior. In this way, the formula "We have always done it this way" gradually displaces the written rules and supplants normative discipline with group habit.

The broken windows theory and the normalization of deviance are mutually complementary concepts that describe one and the same fundamental process from different perspectives.

The broken windows theory emphasizes visual signals and their impact on the behavior of individuals entering a given environment. It explains how the environment shapes behavior from the outside inward: the external signs of disorder signal weakened control and encourage violations, or at least lower the threshold of restraint against committing them.

The normalization of deviance describes the reverse process — from the inside outward: how the internal culture of the organization gradually redraws the boundaries of the permissible, without the participants realizing that they are already operating outside the original standard. Persons outside the organization (third parties) may classify a given behavior as unacceptable, but to the internal participants it already appears normal because it corresponds to their internalized attitudes.

Applied jointly, the two theories provide a comprehensive explanatory framework for the processes of disciplinary erosion: visible disorder simultaneously signals weakened control to newcomers and reinforces the normalization of deviance among the existing members of the organization.

Military organizations are environments in which the broken windows theory possesses considerable analytical value owing to a number of structural characteristics. It should not be mechanically transposed from the urban environment to the military environment, but it offers a useful perspective for the analysis of the disciplinary environment, the command climate, and the role of visible standards.

The hierarchical structure characteristic of the military environment means that the behavior of commanders constitutes a visible signal that is reproduced down the chain of command. The toleration of a violation by a commander often functions as a more powerful practical signal than a series of written orders demanding compliance with discipline. To this is added the physical environment of the military formation: barracks, motor pools, staff offices, weapons-storage facilities, which is immediately visible and communicates with the service members. An uncleaned unit area, a disorderly warehouse, the improper wearing of the uniform, or defective equipment may function as the military equivalent of a broken window. Military service presupposes the intensive integration of new and experienced service members, in the course of which the newcomers rapidly assimilate the actual, rather than merely the formal, norms of behavior.

The armed forces constitute a total institution in the sense of an organization claiming comprehensive control over its members, including their behavior, dress, gestures, and public image — a concept formulated in the classical work of Erving Goffman [8]. It is precisely this total character that renders the visible public behavior of service members a particularly informative indicator: it manifests the degree to which the institution actually exercises the control it claims. Visible behavioral deviations in the public sphere may likewise function as a sign of broken windows. The careless wearing of the uniform, the demonstrative disregard for saluting, or the systematic failure to meet physical standards do not automatically constitute evidence of operational unpreparedness, but they may serve as early indicators of declining standards and weakening command control.

The mechanism through which the toleration of minor violations may escalate into systemic disciplinary breakdown may be described as a chain of six successive phases.

In the first phase — initial deviation — a seemingly insignificant violation appears: lateness by a few minutes, an unbuttoned button on the uniform, a missed inspection. The commander elects not to react, regarding the violation as inconsequential.

In the second phase — signaling — the absence of a reaction is read by the other service members as an indication that the standard has already shifted, or at least that its enforcement is conditional.

In the third phase — normalization — the deviation is repeated and begins to spread. Both veteran and newly assigned service members gradually come to perceive it as standard practice rather than as an exception.

In the fourth phase — escalation — the tolerated minor violations generate a self-reinforcing environment in which the threshold of the permissible shifts progressively and comes to encompass increasingly substantial deviations.

In the fifth phase — withdrawal of control — disciplined service members become demotivated. They either adapt to the lowered standard or cease to expend effort in maintaining order, since they observe that order is not being defended consistently. Inaction is exhibited on the part of both the command and the rank-and-file personnel.

In the sixth phase — critical event — the accumulated erosion materializes in a serious incident, a mission failure, or the destruction of command trust.

This chain of successive toleration of minor violations in peacetime bears a direct relation to the combat preparedness of the troops, since it is precisely in the everyday environment that the attitude toward the standard and toward its obligatory character is formed.

The commander who consistently enforces the requirements concerning appearance and behavior in the everyday public environment cultivates an organizational disposition for the consistent enforcement of combat standards as well. Conversely, the commander who tolerates everyday violations forms a disposition of selective enforcement — destructive precisely under conditions of combat stress. The mechanism operates

symmetrically: the organizational habit cultivated in the everyday environment is carried over into the crisis environment as well.

When minor deviations from the standard are repeated without consequences, the threshold of tolerated deviation gradually rises. The careless wearing of the uniform is not equivalent to failure in the execution of a combat mission, but it may be part of the same cultural pattern of declining standards. By analogy, the systematic neglect of the outward manifestations of discipline does not automatically denote the non-execution of orders, but it creates an environment in which the obligatory character of the standard appears increasingly conditional. Crises rarely occur abruptly; they are typically the result of a prolonged process of accumulation of normalized minor deviations.

A commander who does not exercise his authority in respect of publicly visible everyday violations conveys nonverbal signals to his subordinates that his requirements are conditional and selective. Such signaling is devastating to command authority — precisely the authority upon whose predictability and consistency the execution of orders in critical situations rests.

Of particular significance in this context is the role of the non-commissioned officer corps as the first line of disciplinary control. By analogy with the broken windows theory in its original form, non-commissioned officers are the functional equivalent of the permanent police patrol: their daily presence, immediate observation, and prompt reaction to deviations constitute the primary mechanism for the maintenance of order within the immediate organizational environment.

The public image of the service member is a directly observable indicator of the disciplinary state of the armed forces. Its principal components — the tidiness of dress, physical condition, the rendering of salutes, and conduct in public — may be regarded as functional proxy indicators of the quality of organizational control and of the actual presence of disciplinary standards.

Military dress fulfills a functional, identificatory, and symbolic role simultaneously. The manner in which the uniform is worn in the public sphere constitutes one of the most typical examples of a broken window within the military organization. A carelessly worn uniform — disheveled, unbuttoned, lacking the prescribed elements (for instance, without headgear) — represents not only a visible violation of the normative requirements but also a signal to the other service members that the rules may be treated as optional. Particularly indicative is the practice of daily wearing of field (camouflage) dress in an urban setting without operational necessity, since it signals not functionality but a lowered institutional standard.

Physical fitness is a normatively established requirement and a condition for the continuation of military service under Article 187, paragraph 1, of the Law on Defense and the Armed Forces [4]. The visible physical condition of the service member in the public sphere is a directly observable indicator of compliance with these standards. As an organizational broken window, the systematic and publicly visible non-compliance with the physical requirements may operate on three levels: at the individual level, as a sign of reduced readiness; at the command level, as a signal of weakened control over the standards; and at the institutional level, as a factor undermining public trust in the combat capability of the armed forces. The effect is particularly

unfavorable when such a condition is visible among the officer and non-commissioned officer corps, since these categories are required to serve as exemplars.

The rendering of a salute — the greeting addressed to a service member of higher rank — is an immediately visible test of the functioning of the chain of command. It is not a ceremonial anachronism but a public demonstration of the recognition of hierarchy. An army in which the personnel consistently observe the requirements of saluting and military courtesy in the public sphere demonstrates a functioning hierarchy. Conversely, an army in which these requirements are systematically neglected in public demonstrates an erosion of the hierarchical order.

Essential is the distinction between formal and conscious discipline. Disciplined behavior exhibited solely within the confines of military installations and only under direct supervision constitutes formal discipline. Disciplined behavior in public space, in the absence of direct control, is a hallmark of genuinely internalized discipline. It is precisely this latter discipline that constitutes the precondition for the execution of orders in a combat environment under disrupted communications, upon the loss of commanders, and under extreme psychological pressure. Public behavior is a test of precisely this internally assimilated discipline.

The Law on Defense and the Armed Forces of the Republic of Bulgaria establishes the legal framework of military discipline. Article 242 of the Law defines the types of violations of military discipline; with the most recent amendments, non-compliance with the ethical rules of conduct of service members has been expressly included as a violation giving rise to grounds for disciplinary liability.

From the perspective of the broken windows theory, the normative system establishes the formal norms and the mechanisms of monitoring. Its effectiveness, however, also depends on the third element — signaling, that is, on the actual readiness of commanders to apply the disciplinary instruments consistently and in cases of minor violations as well. A norm that is not applied visibly and predictably gradually loses its disciplining force.

On 22 July 2025, the new Regulations on Military Service of the Armed Forces of the Republic of Bulgaria entered into force [5]. They replaced the Regulations that had been in force since 2008 [6]. The new Regulations were developed in the context of the Armed Forces Development Plan up to 2026 and reflect the restructuring carried out in a significant portion of the armed forces.

Pursuant to Article 1, paragraph 2, of the new Regulations, they determine the rights and duties of service members concerning the organization and execution of military service in garrison areas and beyond them, during participation in missions, as well as the procedure for conducting ceremonies involving troops. Article 4 defines military service as a complex of continuous activities, rules, and norms directed at ensuring the fulfillment of the tasks of the armed forces. Article 5 defines military order as a system of activities and norms directed at ensuring the conditions for the equipping and maintenance of military installations, the implementation of the daily schedule, the observance of the relationships among service members, and the requirements concerning their appearance.

Particularly indicative is the regulation of the physical environment and appearance in Article 18, which governs the elements of the areas of military formations, as well as in Articles 24–26, which contain the requirements concerning the wearing of uniform clothing and distinctive insignia. These provisions bear a direct relation to the broken windows theory, since they establish the standard of visible order, the maintenance of which constitutes the first line of defense against disciplinary erosion.

This theoretical framework permits the derivation of a model for the prevention of disciplinary erosion within military organizations.

By analogy with Bratton's policing approach in New York, the commanders of military formations may apply a systematic visual audit of the environment in the units under their command. Such an audit should encompass at least three dimensions: the physical dimension — the condition of premises, motor pools, warehouses, equipment, and checkpoints; the behavioral dimension — punctuality at formations and duty assignments, compliance with the requirements concerning appearance, uniform, saluting, and military courtesy; and the communicational dimension — the tone of address, the manner of reporting incidents, and the readiness of subordinates to signal problems.

The principal countermeasures should include: the cultivation of a strong safety culture grounded in trust and shared values — as substantiated in detail in the works of James Reason on the management of organizational risks [10]; the maintenance of a state of chronic unease, by means of periodic safety stand-down days and cross-training; and the construction of a just culture that distinguishes unintentional errors from the irresponsible non-observance of the rules. These approaches, however, should be adapted to the particularities of military service and not mechanically transposed from civilian high-risk organizations.

A strong safety culture presupposes an environment in which every service member, regardless of his or her position within the hierarchy, feels both obligated and empowered to signal potential risks, without fearing that a well-intentioned warning will be treated as disloyalty. Such an environment is constructed through consistent leadership behavior, transparent communication, and a clearly demonstrated priority accorded to safety and readiness over the formal reporting of tranquility.

Chronic unease signifies the purposeful maintenance of professional vigilance even during periods of apparently normal functioning. Rather than treating the absence of incidents as proof that the system is safe, organizations should consistently assume that latent threats exist, awaiting favorable conditions to manifest themselves. This approach is characteristic of so-called high-reliability organizations, which operate in high-risk environments yet maintain a low frequency of accidents precisely owing to a disciplined suspicion toward apparent calm — a phenomenon systematically investigated in the works of Weick and Sutcliffe [11].

Periodic safety stand-down days represent a planned suspension of current activity, during which teams analyze accumulated experience, review procedures, and openly discuss problematic situations. Cross-training complements this practice, since it enables service members to familiarize themselves with the functions and limitations of their colleagues in other sections,

thereby broadening perspective and facilitating the recognition of risks that are invisible within the confines of narrow specialization.

Lastly, a just culture, in the sense developed by Sidney Dekker [12], introduces a clear and predictable framework for the evaluation of human errors. It requires the distinction between: the unintentional error, committed notwithstanding the conscientious efforts of the service member; risk-taking behavior, arising from an underestimation of danger; and the deliberate violation, associated with the conscious disregard of established rules. Only the last of these categories justifies a disciplinary sanction in the full sense, while the first two should also be employed as occasions for organizational learning. Without such predictability, any system begins to incentivize the concealment, rather than the reporting, of errors.

The broken windows theory in the organizational context acquires particular depth when applied to the behavior of the leaders themselves. A commander who tolerates his own violations transmits a twofold signal: that the standards are of negligible importance, and that control has weakened. Conversely, small but consistent actions on the part of the commander demonstrating personal adherence to the standard exert a disproportionately large influence on organizational culture.

When a leader disregards a rule he has himself imposed upon his subordinates — irrespective of whether it concerns lateness to a briefing, a missed mandatory inspection, or non-observance of an established protocol — the subordinates rarely perceive this as an isolated episode. They read it as a tacit shifting of the standard. If the commander does not wear a helmet and gas mask after having required this of all others, the message is unambiguous: the rules exist more for form than for substance. The effect is multiplied down the hierarchy, since each successive leadership echelon begins to perceive the deviation as tacit permission to lower its own standard as well.

The psychological mechanism underlying this dynamic is convincingly explained by the social learning theory of Albert Bandura [9], according to which persons model their behavior above all on the actions, rather than on the words, of authority figures. When a discrepancy exists between the declared expectations and the observed behavior of the leader, the subordinates follow the behavior, not the declaration. From this arises the erosion of trust — a process whereby each successive inconsistency between word and deed progressively renders the formal rules meaningless and transforms written procedures into hollow bureaucracy.

The reverse direction of influence is no less powerful. The commander who conspicuously observes even the smallest requirements — who arrives first, who inspects his personal equipment in accordance with the established procedure, who openly acknowledges his own mistakes — creates an environment in which the standards are perceived as living and obligatory. These seemingly minor gestures function as symbolic markers that continuously reaffirm the value framework of the organization. Like the well-maintained façade in the original theory, they signal that someone is in fact watching, cares about order, and defends it.

This effect is particularly illustrative in crisis situations. When, acting under pressure, the leader maintains adherence to

the established procedures rather than circumventing them in the name of speed or convenience, he transmits the strongest possible message: standards are not a luxury for tranquil times, but precisely an instrument for the overcoming of difficulties. Conversely, if at the first difficulty the commander himself violates the protocol, the entire system of rules is revealed as ornamental, valid only under favorable conditions.

Ultimately, the broken windows theory, applied to leadership behavior, reveals a fundamental truth about organizational culture: it is formed not by what is written in the manuals and directives, but by the daily, visible, and consistent actions of those who stand at the apex of the hierarchy. Every small concession by the leader is a crack in the window; every small manifestation of discipline is a timely repair that prevents further destruction.

The criticism of the broken windows theory in the context of policing — more specifically, the danger of over-repression — is relevant to the military context as well. The application of the theory does not signify zero tolerance in the sense of the mechanical punishment of every minor violation. In a military environment, this signifies that the commander should respond to every violation, but the response must be proportionate, consistent, and formative, rather than merely punitive. It is consistency, and not maximum severity, that constitutes the decisive factor in the maintenance of a healthy disciplinary environment.

The transposition of the theory from the urban environment to the military organization is not free of challenges. Military organizations differ from urban communities in several essential parameters: membership is institutionalized, the hierarchy is formal and legally established, control is structured and multilayered, and sanctions are normatively regulated. These differences entail that the environment within the military organization is not confined to the material setting but also encompasses the organizational culture, the command climate, and the mechanisms of selection, training, and socialization.

One of the principal dangers is the risk that disciplinary control may degenerate into an instrument of harassment, formalism, or the suppression of constructive criticism. It is precisely for this reason that any invocation of the broken windows theory in a military context must be accompanied by clear boundaries between the maintenance of the standard and the abuse of power.

As in the original criminological discussion, the link between the toleration of minor violations and the occurrence of serious incidents in a military environment is correlative rather than strictly causal. Consequently, the theory should be regarded as an element of a broader explanatory framework rather than as a sole and self-sufficient causal chain. Its strength lies not so much in the promise of absolute causality as in its capacity to capture the early signals of organizational erosion.

IV. CONCLUSION

The broken windows theory of Wilson and Kelling, supplemented by Diane Vaughan's concept of normalization of deviance, provides a valuable analytical and practical framework for understanding and counteracting the processes of disciplinary erosion within military organizations.

The theory offers an explanatory model of the mechanism through which the toleration of seemingly insignificant violations gradually weakens the organizational culture. Furthermore, it emphasizes the significance of the physical environment and of visual signals as indicators of the state of discipline — an aspect elaborately regulated in the Regulations on Military Service. At the same time, the theory substantiates the necessity of a consistent, albeit proportionate, response to all violations — not so much for the sake of the sanction itself as for the signal that the response transmits to the entire organization.

The normative framework of the Republic of Bulgaria — the Law on Defense and the Armed Forces, its implementing regulations, and the Regulations on Military Service — provides an adequate legal basis for the maintenance of military discipline. The inclusion of non-compliance with the ethical rules of conduct as a violation of military discipline under Article 242 of the Law represents a step in the proper direction. The legal framework in itself, however, is insufficient unless it is supported by consistent command practice and by an organizational culture that renders the standards visible and effectively obligatory.

Of particular importance is the application of the derived model with respect to the officer corps. By virtue of his rank and in accordance with the established traditions of military service, the officer is the bearer and transmitter of a value system that far exceeds the framework of the specific functional duties. The visible conduct of the officer in public space — the observance of the requirements concerning appearance, military courtesy, the maintained physical fitness, and adherence to the disciplinary standards outside any directly assigned duty — shapes the perception, both of the subordinates and of society, of the essence of officer's honor. The toleration of minor personal deviations on the part of an officer, even when not directly connected with the exercise of command authority, operates as a broken window within the officer corps and gradually undermines the overall level of the disciplinary standard. Conversely, the consistently demonstrated personal adherence to the requirements on the part of the officers in any public situation functions as a daily instrument for the preservation of officer identity and for the construction of an integral military culture in which discipline is a personal responsibility rather than an externally imposed obligation.

The challenge remains precisely in the sphere of organizational culture — in the readiness of commanders at every level to repair the broken windows in a timely manner, consistently, and without ostentatious formalism, before small cracks turn into wide breaches. In this sense, discipline is not merely a matter of sanction, but above all a matter of a daily maintained standard that is seen, applied, and defended.

REFERENCES

- [1] Wilson, J. Q., Kelling, G. L. Broken Windows: The Police and Neighborhood Safety // *The Atlantic Monthly*. — 1982. — Vol. 249, No. 3. — P. 29–38.
- [2] Harcourt, B. E. *Illusion of Order: The False Promise of Broken Windows Policing*. — Cambridge, MA: Harvard University Press, 2001.

[3] Vaughan, D. The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. — Chicago: University of Chicago Press, 1996.

[4] Law on Defense and the Armed Forces of the Republic of Bulgaria. State Gazette, No. 35 of 12 May 2009, as last amended State Gazette, No. 1/2026.

[5] Regulations on Military Service of the Armed Forces of the Republic of Bulgaria. Approved by Order No. OH-618 of 27 June 2025. State Gazette, No. 58 of 18 July 2025, in force as of 22 July 2025.

[6] Regulations on Military Service of the Armed Forces of 2008. State Gazette, No. 75 of 26 August 2008. Repealed — State Gazette, No. 58 of 18 July 2025.

[7] Implementing Regulations of the Law on Defense and the Armed Forces of the Republic of Bulgaria. Adopted by Council of Ministers Decree No. 46/2010.

[8] Goffman, E. Asylums: Essays on the Social Situation of Mental Patients and Other Inmates. — New York: Anchor Books, 1961.

[9] Bandura, A. Social Learning Theory. — Englewood Cliffs, NJ: Prentice-Hall, 1977.

[10] Reason, J. Managing the Risks of Organizational Accidents. — Aldershot: Ashgate, 1997.

[11] Weick, K. E., Sutcliffe, K. M. Managing the Unexpected: Sustained Performance in a Complex World. 3rd ed. — Hoboken, NJ: Wiley, 2015.

[12] Dekker, S. Just Culture: Balancing Safety and Accountability. 2nd ed. — Farnham: Ashgate, 2012.

[13] Kelling, G. L., Coles, C. M. Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities. — New York: Touchstone, 1996.

Cultural Parasitism: The Transfer of Foreign Cultural Models as a Threat to National Security

Sabin Sabev

Branch in Veliko Tarnovo
University of Agribusiness and Rural Developments
Plovdiv, Bulgaria
ssabev@uad.bg

Abstract - The present study employs the biological metaphor of parasitism as a heuristic analytical tool, and not as a descriptive or normative characterisation of human beings or communities. The author explicitly emphasises that the analogy refers to systemic-functional models of cultural-institutional interaction, and not to individuals or to ethnic, religious or national groups. In biology, parasitism is a form of symbiosis in which one organism – the parasite – extracts resources from another organism – the host – thereby progressively weakening its viability. When the parasitic load exceeds a critical threshold, the host perishes, and frequently the parasite itself perishes with it. This biological analogy proves heuristically applicable to the analysis of processes observed in contemporary European societies: the large-scale and unregulated influx of cultural models that are fundamentally incompatible with the value system of the host society operates according to the same destructive logic. The foreign cultural model does not adapt to its environment; rather, it reshapes that environment, exhausts its institutional resources, and undermines its capacity for self-reproduction.

The paper examines the transfer of foreign cultural models from migrant communities not as a neutral social process, but as a potential threat to national security in its societal dimension. The study is limited to cases of non-integrated communities with persistently incompatible normative systems, and explicitly distinguishes such cases from: refugees from active military conflicts (Ukraine, Syria), persons fleeing totalitarian regimes (Afghanistan, Iran), and economic migrants with demonstrated capacity and willingness to integrate. The territorial scope of the study covers primarily Germany, France, Sweden, Denmark and the United Kingdom in the period 2010 – 2024.

KEYWORDS: *societal security, migration, cultural integration, parallel societies, national identity*

1. INTRODUCTION

In recent years, Europe has been confronted with a challenge that cannot be reduced to economic indicators, humanitarian obligations or police statistics. This challenge is of a civilisational order – a question concerning the capacity of the societies of the “Old Continent” to preserve their cultural, value-based and institutional foundations under conditions of an unprecedented scale and pace of incoming foreign cultural models. For decades, this process has been presented as neutral, even beneficial – as “enrichment”, “diversity”, “multicultural dialogue”. Europe is known for its tolerance towards all religions, political beliefs and cultures. Today, when the consequences of such an approach are visible on the streets, in the statistics and in the institutions of nearly every Western European state, it is time for a more honest and uncompromising assessment.

1.1. Object and subject of the study. The object of the study is the processes of cultural-institutional interaction between European host societies and non-integrated migrant communities in the period 2010 – 2024. The subject of the study is the systemic-functional mechanisms through which incompatible cultural models affect the societal security of host states.

1.2. Research aim. The aim of the study is to analyse the applicability of the biological concept of parasitism as a heuristic analytical tool for the investigation of processes of cultural-institutional incompatibility, without transferring this tool onto individuals or groups of people.

1.3. Research questions. The study seeks to answer the following questions: (1) Under what structural conditions does the transfer of foreign cultural models turn from “enrichment” into a systemic threat to the societal security of the host state? (2) What are the measurable institutional indicators of such adverse impact? (3) What lessons applicable to Bulgaria can be drawn from the experience of Western Europe?

1.4. Working hypothesis. The author maintains the hypothesis that, when four conditions are simultaneously present – a scale of migration exceeding the integration capacity; fundamental incompatibility of the transferred normative systems with the liberal-democratic order; political and

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.68>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

ideological factors suppressing the host society's defensive mechanisms; and the formation of stable parallel structures – the process of cultural transfer shifts from an enriching one into a dysfunctional one and threatens the societal security of the host state.

1.5. Tasks of the study. To achieve this aim, the following tasks have been set:

- (1) theoretical justification of the heuristic use of the biological analogy with explicit recognition of its limits;
- (2) identification of the structural conditions under which cultural transfer shifts from enriching to dysfunctional;
- (3) comparative review of the experience of selected Western European states;
- (4) formulation of conclusions applicable to the Bulgarian context.

In biology, parasitism is a form of symbiosis in which one organism – the parasite – extracts resources from another organism – the host – gradually weakening its viability. When the parasitic load exceeds its critical threshold, the host perishes, and along with it, usually, the parasite itself. The biological analogy proves surprisingly accurate in analysing the processes observed in contemporary European societies: the mass and unregulated incursion of cultural models fundamentally incompatible with the value system of the host society operates according to the same destructive logic. The foreign cultural model does not adapt to the environment in which it finds itself; rather, it attacks, reshapes and exhausts the institutional resources of that environment and undermines its capacity for self-reproduction. An important methodological clarification: throughout the present paper the term “parasitism” describes relations between cultural-normative models and institutional systems, and not relations between human beings. People are never parasites; only abstract institutional practices of refusal to integrate can be parasitic. In this sense, migrant communities manifest themselves as parasites within the hospitable European community.

Categories of migrants and their differentiation. In the present study, the term “migrant communities” is not used as a homogeneous category. The following groups are explicitly distinguished:

- (a) refugees from active military conflicts (e.g., from Ukraine after February 2022, from Syria in the period 2011 – 2020) – often with high integration potential and similar value systems;
- (b) persons fleeing totalitarian or authoritarian regimes (e.g., from Afghanistan after 2021, from Iran) – with mixed integration potential;
- (c) economic migrants from states with similar normative systems (e.g., from Eastern European countries, Asian states with a high human-development index) – traditionally making a high contribution to the host society;
- (d) communities with stable parallel normative structures – the specific object of the present study.

Only the last category is the subject of the critical analysis; consideration of the first three categories is beyond the scope of

this paper. A further characteristic of these communities is that they profess religious beliefs different from the predominant religion of the host state.

Migration is a historical fact and an enduring part of the development of human civilisation. No analysis can deny that the controlled migration of persons capable of, and willing to, integrate has been, and continues to be, a source of renewal and development for host societies. Many Bulgarians migrated from the Aegean region into the present-day borders of Bulgaria. Bulgaria received and sheltered thousands of Armenian refugees who managed to escape the brutal massacres in Turkey. The problem lies not in the movement of people, but in the transfer of value systems that are structurally incompatible with the foundational principles of the liberal-democratic order – individual liberty, gender equality, freedom of speech, freedom of belief, tolerance of difference, and the rule of law. When these value systems do not merely exist as personal beliefs but become institutionalised in parallel communities that refuse to recognise the norms of the host society, the process ceases to be migration and becomes colonisation from within.

2. MATERIALS AND METHODS

2.1. Data sources. The study draws on an analysis of the following types of sources:

- (a) official statistical data of Eurostat on migration, employment and social inclusion in the period 2010 – 2024;
- (b) publications of the Organisation for Economic Co-operation and Development (OECD);
- (c) official reports of the European Commission and the European Parliament on issues of migration and integration;
- (d) national reports of the German Federal Office for Migration and Refugees (BAMF), of Statistics Sweden (SCB), of the French INSEE and of the British ONS;
- (e) publications of the Center for the Study of Democracy (Bulgaria);
- (f) peer-reviewed academic literature in the fields of security studies, migration studies and integration studies.

2.2. Methods. The following are applied:

- (1) analytical method – to decompose the phenomenon under study into constituent elements and to identify key mechanisms;
- (2) comparative method – to juxtapose the integration policies and outcomes in the selected Western European states;
- (3) secondary analysis of statistical data – to assess the empirical manifestations of the processes under examination;
- (4) method of analogy (heuristic application of the biological concept of parasitism), applied with explicit acknowledgement of its limitations.

2.3. Critical reflection on the methodological limitations of the analogy. The author is aware that analogy between biological and social systems carries the risk of logical fallacies. Social

systems differ substantively from biological ones: they involve volitional and conscious actors, behavioural patterns are plastic and amenable to change, and normative frameworks are subject to democratic deliberation and revision. For this reason the analogy is used solely as a heuristic instrument that helps to discern the structure of the process, and not as a strict causal explanation. The analogy is applied according to the following rigorous criteria of comparison:

- (1) extraction of resources without proportionate contribution – comparable with socio-economic indicators;
- (2) formation of self-reproducing structures – comparable with parallel communities;
- (3) suppression of the “host’s” defensive mechanisms – comparable with institutional dysfunctions.

Beyond these three dimensions the analogy is not, and should not be, applied.

2.4. Period and territorial scope. The study covers the period 2010 – 2024 – an interval in which the consequences of the migration wave of 2015 – 2016 in the EU manifested themselves most clearly. Territorial scope: Germany, France, Sweden, Denmark, the United Kingdom (as reference cases) and Bulgaria (as a contextual case for the application of the conclusions).

2.5. Limitations of the study. The present study is theoretical-analytical in character; it does not offer an original empirical investigation, but rather a secondary analysis of publicly available data and literature. The author does not claim exhaustiveness for the comparative analysis, nor statistical significance for the conclusions. The aim is to propose an analytical framework that may serve as a basis for further empirical research.

3. MAIN BODY

In the biological sciences, classical parasitology distinguishes several phases of parasitic invasion: penetration into the host organism; adaptation to the internal environment and evasion of the immune response; extraction of resources for the parasite’s own reproduction; and, at sufficient load, functional impairment or destruction of the host. An effective parasite “masks itself” – it avoids recognition by the immune system and suppresses the organism’s defensive reactions.

This biological logic finds striking parallels in the social processes accompanying mass non-integrated immigration. The transferred cultural and civilisational model penetrates the host society through migration flows, resists integration by preserving its own structures and norms, extracts resources from the host’s social system – healthcare, education, social benefits without proportionate contribution – and, on reaching a critical mass, transforms the environment in its own image, weakening or destroying the institutional and value-based capacity of the host society. It is reiterated: the term “transferred cultural model” denotes an institutional-normative structure, and not the individuals who carry it. The key element of the parasitic logic is “masking”: political correctness, the understanding that within the framework of one society multiple cultural communities can and should coexist, each preserving its specific values, norms,

language and traditions, without any requirement to adapt them to the culture of the majority, and the fear of accusations of xenophobia, function as immunosuppressants that suppress the natural defensive response of the society. The logic of the analogy is as follows: just as the biological parasite survives because it suppresses the host’s immune response and renders it incapable of defending itself, so cultural parasitism develops unhindered when society is deprived of the very possibility of naming the problem without being morally stigmatised. Society sees the symptoms but is forbidden from making the diagnosis.

One of the clearest manifestations of the parasitic logic is the formation of so-called “parallel societies” – closed communities in which immigrants reproduce the institutional and value-based structure of their place of origin without integrating into the host society. The term entered European political debate from Germany and is used to describe neighbourhoods and communities in which national legislation has effectively been replaced by alternative normative systems – Sharia law, clan justice, kinship law.

Empirical indicators. According to the official reports of the German Federal Office for Migration and Refugees (BAMF) and the analyses of the German Economic Institute (IW Köln), a number of neighbourhoods in cities such as Berlin (Neukölln), Duisburg (Marxloh), Bremen (Gröpelingen), and others, exhibit persistent characteristics of cultural-institutional isolation: a consistently lower rate of language proficiency, a higher dependence on social transfers, a lower rate of completion of secondary education, and elevated rates of recorded crime relative to the city averages [1]. Parallel societies are characterised by low rates of intermarriage between the immigrant population and the majority, by functional isolation from the institutions of the host society – their own courts, media, educational structures – by sustained resistance to acquiring the language and cultural norms of the host, by intra-community pressures sanctioning attempts at integration, and by a high degree of dependence on the host society’s welfare system without proportionate contribution through labour and the payment of taxes and dues [2].

High-trust societies – such as the traditionally Scandinavian ones – function on the basis of an unwritten social contract: each contributes when, and with whatever, he or she can, and takes only what is necessary. The arrival of cultures in which the welfare system is perceived not as a shared resource but as an object for exploitation undermines the very foundation of this contract [3]. When trust is replaced by suspicion, the foundation of the welfare state collapses.

Since 2015, the Swedish police (Polismyndigheten) has periodically published reports on the so-called “particularly vulnerable areas” (särskilt utsatta områden), in which characteristics consistent with the description of parallel societies are observed: a concentration of population of immigrant origin with a low integration index, a strong influence of alternative normative structures, hindered access for state institutions, and elevated levels of criminality. The specific figures and statistical indicators for the relevant periods are to be cited by the author on the basis of the reports of Polismyndigheten [4].

The arrival of cultural models that not only fail to adapt but actively contest the basic values of the host society – gender equality, tolerance, freedom of speech, the rule of law – constitutes a direct threat to national security. The parasitic

analogy is precise: the foreign organism does not merely exist within the body of the host – it replaces the host's tissues with its own.

The process is deepened by what is termed “demographic inertia”. Under this dynamic, immigrant communities have markedly higher fertility rates than the indigenous population and the demographic balance gradually shifts.

Non-integrated communities form closed electoral blocs vulnerable to manipulation by the clan and religious structures within them. Political parties, instead of struggling for integration, compete for the support of these blocs through concessions (especially during elections) which further entrench the parallel structures.

When internal institutions (police, courts, the educational system, regulators) are compromised – through the political influence of non-integrated communities, through pressure for “cultural sensitivity” which de facto amounts to non-enforcement of the law, or through fear of accusations of racism – the state loses the capacity to protect its own citizens. The parasite has reached the host's immune system.

In what does the weakening of institutions consist:

The principal manifestation lies in the direct political influence of non-integrated communities. When closed immigrant groups form electoral blocs, politicians become dependent on their votes. Instead of insisting on the enforcement of the law within these communities, they make concessions – tolerating parallel normative systems, turning a blind eye to violations, appointing “convenient” persons to key positions. The institution formally exists, but in reality serves alien interests.

The second aspect is the pressure for “cultural sensitivity”. At first glance this sounds reasonable – respect for differences. After all, the motto of the European Union is “United in Diversity”. In practice, however, something else often hides behind this phrase: the police do not enter certain neighbourhoods so as not to be accused of discrimination, social services do not intervene in cases of forced marriage or domestic violence because that is “their culture”, schools grant exemptions from general rules under the pretext of cultural differences. The result is that the law is applied selectively – strictly to the majority, indulgently to the parallel communities.

The most powerful of the three mechanisms is the fear of accusations of racism. The civil servant, the police officer, the teacher, the social worker – each of them knows that any action taken against a member of an immigrant community risks public stigmatisation, the loss of one's career, and exposure to a media campaign. This fear paralyses institutions more effectively than any external pressure.

The ultimate conclusion is that, when all three mechanisms operate simultaneously, the state finds itself in a paradoxical position: it continues to exist formally, with its institutions, laws and budgets, but has lost the actual capacity to enforce them. Citizens pay taxes for institutions that do not protect them and which, in some cases, even act against their interests in the name of “cultural sensitivity”.

The parasitic model presupposes a unilateral extraction of resources without proportionate contribution. In economic terms this manifests itself in disproportionate dependence on social

transfers – without commensurate fiscal participation and labour contribution; pressure on the educational and healthcare systems; rising costs for security – police, border guards, counter-intelligence; and a loss of investment attractiveness in the neighbourhoods and urban zones in which parallel communities form. The Scandinavian models – traditionally regarded as exemplars of the welfare state – face unprecedented strain precisely because of the incompatibility between a universally accessible welfare system that grants benefits and services to all, without exception, by virtue of mere presence on its territory and irrespective of contribution, on the one hand, and the mass arrival of communities with divergent cultural conceptions of the role of the state, on the other.

Experience demonstrates that the failure of integration is not accidental, but a systemic outcome of the fundamental incompatibility between certain cultural models and the democratic legal order [5]. When immigrant communities import clan solidarity, patriarchal hierarchy, the primacy of religion over secular law, and the collectivist suppression of individual liberty, they do not “enrich” the host society – they erode it from within. It must again be emphasised here that this proposition does not imply that every individual carrier of a given cultural tradition acts destructively. What is at stake are statistically and institutionally measurable tendencies under conditions of an absence of integration policies. The parasite does not contribute to the health of the host but consumes it.

The biological analogy implies that effective counteraction requires recognition (the capacity to identify the threat without ideological constraints), selectivity (distinguishing between migrants capable of integration and carriers of incompatible cultural models), a proportionate response (measures commensurate with the scale of the threat), and the building of immunity (strengthening of national identity, the educational system and the value-based foundation) [6] – [7].

To counter this social parasitism, concrete measures should include: mandatory cultural integration programmes with measurable outcomes and sanctions for non-compliance; limits on the concentration of migrants of the same cultural group in particular neighbourhoods; zero tolerance towards parallel normative systems, with no exceptions on grounds of “cultural sensitivity”; the linking of social benefits to demonstrated integration; and the strengthening of law-enforcement capacity in zones where non-integrated communities are concentrated. All proposed measures should be implemented with unconditional respect for fundamental human rights, with no discrimination on ethnic or religious grounds, and in strict compliance with the European Convention on Human Rights and Article 6 of the Treaty on European Union.

Bulgaria, although not affected by mass non-European immigration to the extent of Western Europe, is vulnerable in two principal respects. As a transit state on the Balkan route, it is exposed to the risks of illegal migration and the potential formation of enclaves. Second, the country is the object of hybrid operations in which migration is used as a tool of pressure – as documented in the report of the Center for the Study of Democracy entitled “Countering Hybrid Threats in Bulgaria” [8].

For Bulgaria, the experience of Western Europe is at once a warning and an opportunity to learn. The early construction of effective institutional immunity – before the critical mass of parasitic load is reached – is significantly cheaper and more

effective than the treatment of an already developed systemic disease.

One of the most substantial yet seldom discussed questions in the debate on mass migration is the moral one. Contemporary political discourse has successfully imposed the notion that any criticism of uncontrolled immigration is a manifestation of moral inadequacy – of racism, xenophobia, or at the very least a lack of empathy. This is perhaps the most effective immunosuppressant, because it attacks not the argument but the moral standing of the one expressing it. Anyone who dares to raise the question of the limits of migration finds himself or herself not a participant in rational dialogue but a defendant before a moral tribunal. Yet, on closer inspection, the moral argument also operates in the opposite direction, and with no less force. Every society has a moral obligation not only to those who arrive from outside, but also to those who are already here – to its own citizens, to their children and grandchildren, to the generations that will inherit the consequences of today's decisions. When a state permits the mass arrival of cultural models that undermine the foundations of its public order, it does not display generosity – it displays irresponsibility towards its own people. Generosity is a virtue only when it does not endanger the survival of the one who exercises it.

There is also another moral aspect that deserves attention: responsibility towards the migrants themselves. When a society admits more people than it can integrate, it does not do them a favour – it condemns them to marginalisation, to life in the ghetto, to unemployment and dependence on social benefits. Genuine humane treatment is not the uncritical opening of the doors but the honest assessment of integration capacity and a consistent policy that ensures that those admitted truly become full members of society and not its peripheral inhabitants. If behind the façade of tolerance there is in fact indifference – “let everyone live as he wishes, so long as it does not affect me” – then the coexistence of different cultures is not a manifestation of respect but of a refusal of engagement. Genuine respect presupposes dialogue, and dialogue presupposes shared rules. When a society refuses to insist on the observance of these rules out of fear of being accused of intolerance, it in fact abdicates its own moral position.

One of the most insidious aspects of cultural parasitism is its temporal logic – the way the consequences accumulate with each successive generation and at a certain point become practically irreversible. The first generation of immigrants, even when it does not integrate, retains a certain awareness of its status as a “guest” in a foreign society. The second generation, however, is already born on the territory of the host state and bears its citizenship, yet is frequently raised entirely within the confines of the parallel community – with its values, its language, its norms. This generation is formally a citizen but factually a foreigner in its own state. The third generation not only does not integrate, but often radicalises its positions – precisely because it senses the painful contradiction between its formal belonging and its real isolation.

This generational effect is of key importance for understanding the problem, because it shows that cultural parasitism is not a self-correcting process. The widespread belief that “in time, everyone integrates” is not only unconfirmed by experience, but is also a dangerous misconception. Under certain conditions – critical mass of the parallel community, geographical concentration, the presence of internal mechanisms

sanctioning integration – time works not for integration, but against it. Every new generation raised within a parallel society is further from the host culture, not closer to it.

The question of irreversibility is perhaps the most uncomfortable one in the entire debate. Is there a point beyond which the process can no longer be reversed? In the biological analogy, the answer is unambiguous: when the parasitic load exceeds a certain threshold, the host perishes regardless of the treatment undertaken. In the social context, the threshold is not so categorical, but it is no less real. We would not wish to imagine what the outcome would be. When parallel communities reach such demographic, economic and political volume that they are able to dictate terms to the host society, the balance of power is irreversibly shifted. For this reason the question of time is so critical. Every year, indeed every month, of delay in undertaking measures does not merely preserve the status quo, but worsens the situation irreversibly. A child born today within a parallel society will, in twenty years' time, be a citizen with the right to vote, but with values formed outside the civilisational perimeter of the host society. The politician who today postpones a decision, in order not to be accused of intolerance, will tomorrow face a problem that no longer admits of a solution.

European host societies find themselves in a state of profound clash between reality and conviction – a contradiction between what they observe and what they are permitted to think. They observe the formation of parallel societies, sense the erosion of social trust, encounter the everyday consequences of failed integration, and yet are afraid to comprehend and to name these phenomena out of fear of social stigmatisation. The internal contradiction is usually resolved in one of two ways: either by adjusting beliefs to fit reality, or by denying reality so as to fit beliefs. The prevailing tendency in liberal societies is the second – denial.

This denial is institutionalised. The media avoid certain topics or present them in sanitised form. The academic milieu isolates and marginalises the researchers who address them. Politicians refrain from raising them, except in the context of electoral campaigns in which populist rhetoric replaces analytical rigour. The result is paradoxical: the more serious the problem, the more difficult it becomes to discuss; the more action is required, the more impossible decision-making becomes. Society resembles a patient who refuses a diagnosis for fear of hearing an unpleasant truth.

This internal contradiction has a further, no less dangerous, consequence: it pushes the debate from the rational space of analytical discourse towards the emotional extremes of populism. When the legitimate concerns of citizens are silenced by leading politicians and “experts” in the media, those concerns do not disappear; they find expression in extreme forms – in movements that replace analytical critique with racial rhetoric, and in parties that offer simple solutions to complex problems. By a cruel irony, it is precisely the refusal of rational debate on the topic of migration that creates the conditions for the rise of the far-right movements which are then themselves used as an argument for further silencing of critical voices. The vicious circle closes.

In order for this imbalance to be resolved in a healthy manner, what is required above all is the restoration of the capacity for open and honest conversation. This means separating analytical debate from moral blackmail. The fact that far-right movements

also criticise migration does not mean that all criticism of migration is far-right. The fact that racists reject multiculturalism does not mean that every rejection of multiculturalism is racism. This elementary logical distinction is the first step towards overcoming the internal contradiction and restoring the analytical capacity of the host society.

There is also a deeper question that is rarely raised: what becomes of a society that systematically suppresses its own instincts of self-preservation? In the biological analogy the answer is known: an organism whose immune system is suppressed is not merely vulnerable to parasites – it is vulnerable to everything. A society that has lost the capacity to distinguish between enriching interaction and destructive invasion is a society in profound crisis – a crisis not of tolerance, but of self-awareness. The restoration of this self-awareness, with a clear understanding of one's own values, one's own boundaries and one's own right to exist, is the most important precondition for any effective policy on migration and integration.

4. LIMITATIONS OF THE STUDY AND DIRECTIONS FOR FUTURE RESEARCH

The present study has several substantial limitations that should be explicitly acknowledged.

First, the methodology relies primarily on analogical and comparative analysis, without an original empirical investigation.

Second, the use of a biological analogy to describe social processes, even when limited to institutional-normative models, carries the risk of unwarranted generalisation and should be regarded as a heuristic instrument rather than a strict explanatory theory.

Third, the comparative analysis is confined to a small number of Western European states and may not adequately reflect other regional contexts.

Fourth, the study does not examine in detail successful integration practices that would offer positive counter-argumentation.

To overcome these limitations, future research could:

- (a) conduct quantitative analyses of correlations between particular integration policies and measurable social outcomes;
- (b) include comparative case studies of successful integration (e.g., in Canada, Australia);
- (c) develop empirical indicators for establishing the “critical threshold” inferred above by analogy;
- (d) investigate the development of the problem in the Bulgarian and Eastern European context.

5. CONCLUSION

The parasitic analogy, applied to the processes of cultural transfer under mass non-integrated immigration, reveals a logic

that is at once clear and disquieting. The analogy applies to institutional-normative models, not to individuals or to groups of people. The parasite – the foreign cultural model, transferred without adaptation – penetrates the body of the host (the receiving society), suppresses its immune system through political correctness and multiculturalist ideology, extracts resources through the welfare systems without proportionate contribution, forms its own structures – parallel societies – which displace the tissues of the host, and at sufficient load destroys the capacity of the host society to function as a cohesive unit.

Of course, the analogy has its limitations: human beings are not micro-organisms, and a society is not a biological organism. A range of immigrant communities integrate successfully and contribute to the development of their host societies. The key question, however, is not whether integration is possible, but under what conditions the transfer of cultural models passes from enrichment to destruction. That threshold is crossed when the scale of migration exceeds the integration capacity of the host society; when the transferred cultural model is fundamentally incompatible with the basic values of the host; when political and ideological factors suppress the defensive mechanisms of the society; and when stable parallel structures form and reproduce themselves [9].

It is essential that the science of security treat cultural parasitism not as a metaphor, but as an analytical instrument enabling the understanding of processes that undermine the cultural and identity-based resilience of European nations. Precisely because the consequences of ignoring the problem are irreversible, and because a parasite, left uncontrolled, ultimately destroys its host, early diagnosis and a decisive immune response are not manifestations of intolerance, but of responsibility for the survival of the host society and its civilisational identity. At the same time, every practical response must, without exception, respect the rule of law, fundamental human rights, and the prohibition of discrimination.

REFERENCES

- [1] Bundesamt für Migration und Flüchtlinge (BAMF), Migrationsbericht 2022. Nürnberg: BAMF, 2023.
- [2] J. Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. London: Routledge, 2006.
- [3] T. Theiler, “Societal Security and Social Psychology,” *Review of International Studies*, vol. 29, no. 2, pp. 249–268, 2003.
- [4] Polismyndigheten, *Lägesbild över utsatta områden – risker, konsekvenser och åtgärder*. Stockholm, 2023.
- [5] V. Bello, *International Migration and International Security: Why Prejudice Is a Global Security Threat*. Abingdon: Routledge, 2017.
- [6] B. Buzan, O. Wæver, and J. de Wilde, *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers, 1998.
- [7] B. Buzan, *People, States and Fear: The National Security Problem in International Relations*, 2nd ed. Boulder, CO: Lynne Rienner, 1991.

[8] Center for the Study of Democracy, Countering Hybrid Threats in Bulgaria. Sofia: CSD, 2023.

[9] O. Wæver, B. Buzan, M. Kelstrup, and P. Lemaitre, Identity, Migration and the New Security Agenda in Europe. London: Pinter Publishers, 1993.

Eco-Leadership and Green Human Resource Management as Drivers of Environmental Security and Critical Infrastructure Resilience

Dafinka Sidova

Department of National and
International Security
New Bulgarian University
Sofia, Bulgaria

ORCID: [0000-0001-6254-2874](https://orcid.org/0000-0001-6254-2874)

Valentin Vasilev

Department of National and
International Security
New Bulgarian University
Sofia, Bulgaria
vvasilev@nbu.bg

Petar Arabadzhyski

Department of National and
International Security
New Bulgarian University
Sofia, Bulgaria
parabadzhyski@nbu.bg

Abstract— The main aim of this paper is to examine the role of eco-leadership and Green Human Resource Management as key drivers for strengthening environmental security and the resilience of critical infrastructure. In the context of increasing environmental risks, climate challenges, and the growing need for the protection of natural resources, organizations responsible for managing critical infrastructure face the necessity of integrating sustainable management practices and innovative leadership models.

The study examines the concept of eco-leadership as a managerial paradigm oriented toward aligning organizational strategic objectives with the principles of sustainable development and environmental security. In particular, it emphasizes the role of Green Human Resource Management as a strategic instrument for fostering an organizational culture grounded in sustainability, environmental responsibility, and the effective governance of human capital.

Furthermore, the research explores the development of green competencies, mechanisms for enhancing employee motivation, the emergence of “green jobs,” and the critical importance of continuous training and organizational development in the construction of sustainable management systems. Within this framework, special attention is devoted to the contribution of the human factor to strengthening the resilience of organizations responsible for critical infrastructure, particularly in contexts characterized by environmental risks and crisis situations.

In conclusion, by identifying key challenges and best practices related to the implementation of eco-leadership and Green Human Resource Management, the paper derives recommendations for sustainable policies and managerial strategies that contribute to strengthening environmental security and critical infrastructure resilience

The paper uses a conceptual research approach based on a narrative review of literature and selected good practices to develop a model linking eco-leadership, Green Human Resource Management and security outcomes.

Keywords - Critical Infrastructure Resilience, Eco-Leadership, Environmental Security, Green Human Resource Management.

I. INTRODUCTION

The topic of environmental security is becoming increasingly important in light of current global climate change, rising environmental threats, and the growing vulnerability of natural resources. It is becoming a crucial component of the Human Security Concept, with the preservation of the environment and the guarantee of sustainable circumstances for human life and societal advancement at its center. [1]

Energy systems, water supplies, transportation networks, and communications are examples of critical infrastructure that is especially vulnerable to the effects of environmental conditions. Serious socio-economic repercussions may result from disruptions to its operation brought on by natural catastrophes, climate change, or environmental crises. In this situation, both national and international security strategically prioritize the resilience of critical infrastructure.

In this process, the human element plays a particularly significant role [2] - [4]. Human resource management should be seen as a strategic tool for creating sustainable companies that can successfully address environmental issues rather than just as an administrative task. This makes it clear that new management techniques must be incorporated, with eco-leadership and Green Human Resource Management standing out among them.

Conversely, eco-leadership is seen as a modern management approach that integrates social responsibility, strategic thinking, and a dedication to sustainable development. It is the development of an organizational culture where environmental values are included into daily operations and decision-making processes [5], [6]. In this way, leaders are crucial in encouraging innovation,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.105>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

sustainable behaviour, and employee engagement. This idea expands on traditional leadership paradigms and offers fresh insights into their thorough analysis and use.

The main contribution of the paper is the development of a conceptual model that integrates eco-leadership, Green Human Resource Management and security-oriented organizational capacities. The model highlights the role of green competencies, employee motivation, psychological resilience and inter-team coordination as mechanisms through which human capital can support environmental security and critical infrastructure resilience.

II. MATERIALS AND METHODS

For the past few years, at both global and national levels, scholarly and expert debates are increasingly intensifying regarding the significance of the eco-friendly orientation of leadership and human resource management. In this context, the relationship between the sustainability of management processes and the assurance of environmental security is directly proportional; that is, as the former strengthens, the latter is correspondingly enhanced.

The study applies a conceptual research approach based on a narrative review of academic publications and selected project documents related to eco-leadership, Green Human Resource Management, environmental security and critical infrastructure resilience. The reviewed sources were grouped into thematic categories: green competencies, employee motivation, green jobs, crisis preparedness, psychological resilience and inter-team coordination. Based on these categories, a conceptual model was developed to explain the relationship between eco-leadership, Green Human Resource Management and security outcomes.

Thus, a key indicator of the effectiveness of eco-leadership is the extent to which environmental human rights are protected in both quantitative and qualitative terms. In particular, these rights encompass equitable and non-discriminatory access to essential natural resources - including land, shelter, food, water, and clean air - which are fundamental to human survival and well-being across both personal and professional domains. Furthermore, the protection of environmental human rights serves as a critical benchmark for sustainable governance and organizational responsibility. In this regard, three core environmental human rights can be distinguished: the right to a safe, clean, healthy, and sustainable environment (including within the workplace); the right to clean and accessible drinking water; and the right to safe, hygienic, and accessible sanitation and working conditions [7].

From that point of view, as Stefanova, Popescu and Vasilev [8] draw the attention, it is important to underline that recruitment, training, performance evaluation, motivation, and staff development are all important aspects of human resource management that incorporate environmental concepts. Moreover, the development of so-called "green competencies", which encompass knowledge, skills, and attitudes connected to environmental preservation, effective resource use, and

sustainable thinking, is a crucial component of Green Human Resource Management [9]. In this context, employee training and development acquire strategic importance, as they support the building of organizational capacity to address environmental challenges.

Another important factor is employee motivation. Therefore, employers who provide suitable incentives for environmentally conscious behavior foster more employee involvement and a deeper sense of commitment to sustainability objectives. Because they are associated with activities that mitigate adverse environmental impacts, so-called "green jobs" are becoming increasingly significant in this process.

Recent developments in Green Human Resource Management have led to the conclusion that Green Human Resource Management helps companies become more resilient and competitive in addition to improving their environmental performance. Furthermore, organizations can more successfully manage risks associated with environmental crises and guarantee long-term stability by fostering a culture of sustainability and engagement. In this sense, it is an integrated management method that systematically integrates sustainable development objectives and environmental principles into every aspect of human capital management [10]. In addition, Green Human Resource Management is becoming a crucial component for improving organizational adaptation, efficiency, and resilience in the face of escalating environmental threats and increased demands on businesses for sustainable operation, especially in important infrastructure-related industries.

Incorporating sustainable values and environmental standards into traditional HR processes is the core of Green Human Resource Management [11], [12]. Consequently, this entails creating a corporate culture where environmental responsibility is ingrained in workers' daily conduct in addition to formally introducing "green" rules.

Important indicative characteristics for identifying Green Human Resource Management can be derived from several of its key features:

- **Green Recruitment and Selection** – this dimension extends the scope of recruitment and selection procedures by incorporating elements related to the overall understanding of environmental challenges faced by organizations and the importance of their activities in addressing these issues. Candidates with sustainable thinking, environmental awareness, and a desire to take part in green activities are becoming more and more sought after by organizations. By incorporating these factors into the hiring process, teams that can support the organization's sustainability goals are formed [13].
- **Training and development of green competencies** is a central element of Green

Human Resource Management. These competences include, among other things, an understanding of environmental dangers and regulations, the ability to use resources efficiently, and attitudes that are focused on sustainable conduct. Building capacity for environmental crisis prevention and response is facilitated by training and development programs Ziolkowska [14], Matura, and Singh [15] highlight in their studies. This is especially crucial for organizations in charge of key infrastructure,

- **Performance appraisal with an environmental focus** involves the introduction of environmental indicators into performance evaluation systems, encouraging employees to actively contribute to sustainability goals, according to Cabral and Dhar [16]. This may include metrics related to waste reduction, energy efficiency, or participation in green initiatives,
- **Motivation and stimulation of green behaviour** – as argued by Gigauro, Vasilev, and Sidova [17], motivational mechanisms play a crucial role in encouraging environmentally responsible behaviour. Financial and non-financial incentives, recognition, and participation in sustainability-oriented projects create conditions for higher employee engagement,
- **Development of “green jobs”** - Afsharbakeshlo, Omidvar and Gigauro [18] affirm that the creation of job positions related to the management of environmental processes and sustainable practices is an important step toward integrating sustainability into the organizational structure. These positions contribute to better resource management and the reduction of environmental risk.

To emphasize, the effectiveness and practical manifestation of eco-leadership are intrinsically linked to the successful implementation of Green Human Resource Management. In particular, leaders who demonstrate a sustained commitment to the principles of sustainable development facilitate the adoption of green practices and the cultivation of an environmentally oriented organizational culture. With this in mind, eco-leadership functions as a critical catalyst that guides, shapes, and accelerates the transformation of human resource management toward a comprehensive model of sustainability-oriented governance.

In an attempt to enrich this research, an ongoing project under the Programme 2021 - 2027 Interreg VI-B Central Europe could be pointed as a good practice – “Resilient, Sustainable and Innovative social Entrepreneurship in Central Europe” [19]. In the core of the project lays the

priority of enhancing digital and green skills of 25 social economy enterprises, as well as fostering management of change attitude, it's expected to trigger a concrete change in peripheral areas ecosystem, leveraging on the social economy potential.

Another good example is a “Enhancing the development of Centers of Vocational Excellence in the Danube Region by fostering competence and skill development, business-education cooperation and transnational networking” [20] project, full completed in 2025. Three public institutions from Hungary, Serbia and Slovenia combine their efforts to foster competence and skill development in high-quality vocational education and training programs with a special focus on green skills and learning competences.

In 2019 a successful project between Hungary and Romania was closed - “Green Skills Platform for Sustainable Employment Development” [21]. The most valuable achievements are related to contributing to increase of the employment in the area by providing employees skills for green companies, improving the business environment through integrated development measures and providing knowledge to employers, managers, entrepreneurs, and potential entrepreneurs to manage (open) more friendly environment businesses.

Organizational sustainability is directly impacted by Green Human Resource Management, especially when it comes to critical infrastructure. Organizations can more successfully identify and manage environmental risks, respond appropriately to emergencies, preserve business continuity, and lessen adverse environmental impacts by developing skilled and engaged human capital. In this sense, Green Human Resource Management functions not only as a tool for sustainable development, but also as an essential component of security systems. On account of the fact that the human factor plays a key role in the prevention, management, and recovery from environmental incidents, which highlights the importance of investments in training, motivation, and development, the following main part of this paper is focused on its role in the resilience of critical infrastructure.

III. RESULTS AND DISCUSSION

In the contemporary context, the resilience of critical infrastructure has traditionally been examined through the lenses of technology, physical security, and financial investment. However, with the increasing severity of environmental risks and climate change, the human factor emerges as the most critical and simultaneously the most vulnerable component of the security system. The human element acts as a resilience multiplier: a well-trained and motivated workforce can significantly enhance the effectiveness of technical and organizational measures [22]. Employees within organizations responsible for critical infrastructure—such as energy, transport, water supply, communication systems, and healthcare services - are not merely executors of technical tasks. They are key

actors whose decisions, actions, and professional behaviour can either prevent or mitigate the consequences of environmental crises. This necessitates a transition from traditional Human Resource Management toward strategic Human Capital Management, shifting from an administrative approach to the development of human competencies, experience, and adaptability [23].

Organizational culture and training play a pivotal role in building long-term resilience. The development of a sustainability-oriented culture implies shared responsibility for environmental security, proactivity in identifying threats, and zero tolerance for behavioural patterns that may compromise vital systems. It is precisely in this context that eco-leadership becomes essential—leaders who demonstrate commitment to environmental values foster trust and inspire employees to adhere to sustainability principles.

Such a culture is cultivated through consistent policies and a continuous learning process. Modern training programs should incorporate regular simulation exercises addressing environmental crises such as floods, wildfires, and energy infrastructure failures. As highlighted by the EU Civil Protection Knowledge Network, the development of these competencies is essential for enhancing preparedness and response to environmental risks [24].

Effective response to environmental crises imposes specific requirements on the human factor that extend beyond technical competence. Several personnel characteristics are of critical importance under conditions of high risk and time pressure. These include situational awareness (the ability to rapidly assess a dynamically changing environment), adaptive decision-making (the capacity to act effectively in situations where predefined plans are no longer applicable), and efficient communication and coordination among multidisciplinary teams (technical, emergency response, environmental, and managerial) involved in crisis management.

A key prerequisite for successful crisis management is the psychological resilience of personnel involved in crisis response, enabling them to withstand stress and maintain clear and focused cognitive functioning.

In addition to the examined components of Green Human Resource Management, this analysis focuses on two aspects that may significantly influence the resilience of critical infrastructure during real environmental crises: psychological resilience of personnel and inter-team coordination.

The first aspect concerns psychological resilience and employee well-being. Workers operating under conditions of high stress, tight decision-making deadlines, and information scarcity during environmental events - such as floods, fires, or failures in energy and water supply infrastructure - must make rapid and appropriate decisions while maintaining cognitive clarity. This necessitates the implementation of well-being, resilience, and mindfulness programs that support employees in coping with psychological pressure during crisis situations [25].

The second aspect relates to real-time coordination among teams. Environmental challenges are rarely addressed by a single isolated team. A key prerequisite is seamless synchronization among technical, emergency, environmental, and managerial units. The introduction of environmental Key Performance Indicators into incentive and reward systems [26] is also crucial, as it aligns employee behaviour with sustainable procedures and ensures accountability for environmental outcomes. Regular simulation exercises involving multiple teams represent an especially valuable tool, as the lack of coordination is often a critical factor in the failure of large-scale incident responses.

These two aspects complement the existing components of Green Human Resource Management by adapting them to the specific requirements of critical infrastructure. In this way, the interconnection between eco-leadership, green human resource management, and the human factor capable of translating sustainability principles into practice is completed. Human potential, systematically developed through contemporary human capital management approaches, is established as the third dimension of the triangle: “environmental security – critical infrastructure – human resources” [4].

In organizations responsible for critical infrastructure, Green Human Resource Management practices can support system security by ensuring that employees are trained to recognize environmental risks, follow emergency procedures, communicate effectively during crises and participate in coordinated recovery actions. Therefore, the human factor should be considered an operational component of infrastructure resilience.

IV. CONCEPTUAL MODEL: GREEN HUMAN RESOURCE MANAGEMENT – ECO-LEADERSHIP – SECURITY AND POLICY, AND MANAGERIAL RECOMMENDATIONS

As a result of the theoretical and practical research, the authors propose a conceptual model Green Human Resource Management - Eco-Leadership – Security (incl. critical infrastructure resilience), shown on “Fig. 1”.

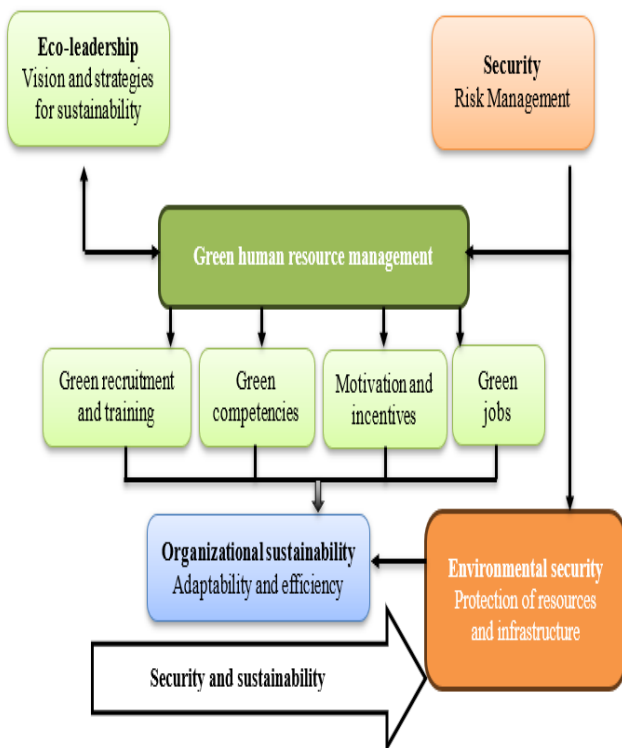


Fig. 1. A conceptual model Green Human Resource Management - Eco-Leadership – Security. (authors' interpretation)

The model shows that eco-leadership and Green Human Resource Management do not function in isolation, but in synergy. Eco-leadership provides the strategic framework and value orientation, while Green Human Resource Management supplies the tools for their practical implementation. As a result, sustainable human capital is developed, which contributes to enhancing organizational security and resilience [27].

The model suggests that eco-leadership provides the strategic direction and environmental values of the organization. Green Human Resource Management translates these values into HR practices such as recruitment, training, performance appraisal, motivation and employee development. These practices contribute to the development of green competencies, employee engagement, psychological resilience and inter-team coordination. These organizational capacities support risk prevention, crisis response and recovery after environmental incidents. As a result, human capital becomes an operational factor in strengthening environmental security and critical infrastructure resilience.

Based on the derived summaries, conclusions, and specific challenges, several key Policy and Managerial Recommendations can also be presented at three levels:

- **At the institutional and organizational level – 1.** Organizations managing critical infrastructure should introduce annual training modules on environmental risk recognition, emergency

response, resource efficiency, crisis communication and inter-team coordination; **2.** Introduction of green skills standards in education and professional qualification systems; **3.** Promotion of public–private partnerships for developing sustainable management practices; **4.** Integration of environmental criteria into all human resources processes (recruitment, performance evaluation, development); **5.** Establishment of internal policies for sustainable human capital management; **6.** Development of training and development programs for green competencies; **7.** Implementation of systems for evaluating employees' sustainability performance,

- **At the leadership and human capital level – 1.** Development of eco-leadership skills through specialized training and coaching; **2.** Encouraging ethical and sustainable decision-making; **3.** Active engagement of leaders as ambassadors of sustainable organizational culture; **4.** Stimulating environmentally responsible behaviour through motivational mechanisms; **5.** Increasing employee awareness and engagement in sustainability goals; **6.** Supporting the development of initiative and innovation in green practices,
- **At the security and risk management level – 1.** Green Human Resource Management indicators should be included in risk management dashboards, including employee participation in environmental training, completion of crisis simulations, compliance with sustainability procedures and contribution to energy and waste reduction targets; **2.** Development of training and response scenarios for environmental crises; **3.** Enhancing organizational readiness and resilience through the human factor.

V. CONCLUSIONS

The significance of eco-leadership and Green Human Resource Management goes beyond corporate responsibility and becomes a strategic issue for security and sustainable development in the context of intensifying climate change, rising environmental threats, and a more complicated global environment. In addition to modifying their technology, organizations in charge of critical infrastructure must change their management approaches by incorporating people as a vital resource for sustainability and resilience.

According to Singh and Kumar [28], and Evangeline [29], the successful integration of eco-leadership and Green Human Resource Management produces a synergistic effect that results in the development of an organizational culture based on accountability, flexibility, and proactive environmental risk management. Human capital participates actively in processes that provide environmental security through the development of green capabilities, involvement, and sustainable behaviour.

It is especially crucial to remember that critical infrastructure resilience cannot be reduced to a technical or

technological problem [4]. It is heavily reliant on the calibre of management and leadership as well as the capacity of enterprises to create a culture of readiness, learning, and flexibility. In this way, Green Human Resource Management becomes a crucial tool for strengthening resilience and lowering susceptibility in uncertain and crisis situations.

In the future, there is a growing need to develop integrated models that link environmental security, human resource management, and strategic leadership into a unified conceptual framework. The practical application of such models could contribute to more effective risk management, enhanced competitiveness, and the creation of long-term value for society.

Future research should empirically test the proposed model through case studies, surveys or interviews with organizations responsible for energy, water, transport, communication or healthcare infrastructure.

In summary, investments in eco-leadership and Green Human Resource Management are essential rather than optional. They serve as the cornerstone for creating ethical, safe, and sustainable companies that can handle the challenges of the future. The conditions for the efficient preservation of environmental resources, the integrity of vital infrastructure, and the preservation of public welfare are exactly established by this integrated approach.

The high practical value of such research lies in its ability to support organizations and public institutions in developing proactive strategies for sustainability, resilience, and crisis preparedness. In an environment characterized by increasing ecological, technological, and social risks, integrated interdisciplinary models can provide a solid foundation for informed decision-making and long-term organizational stability. Furthermore, these approaches contribute to strengthening cooperation between management structures, employees, and society in the pursuit of sustainable development goals.

In summary, investments in eco-leadership and Green Human Resource Management are essential rather than optional. They serve as the cornerstone for creating ethical, safe, and sustainable companies that can handle the challenges of the future. The conditions for the efficient preservation of environmental resources, the integrity of vital infrastructure, and the preservation of public welfare are exactly established by this integrated approach.

REFERENCES

- [1] D. Sidova, "Human Security concerns relating to Environmental Issues" in *Integration of the Western Balkans in NATO as a Guarantee for Regional Stability*. Skopje: Center for International and Development Studies Skopje. ISBN 978-608-245-725-3 2021, pp. 66-79.
- [2] V. Vasilev, D. Stefanova and M. Icheva, "Green Human Resource Management as a Component of Sustainable Organizational Development in Environmental and Natural Economics" in *Environment. Technology. Resources. Proceedings of 15th the International Scientific and Practical Conference*, Vol. 1, 2024, pp. 402–407, [Online]. Available: <https://archive-journals.rtu.lv/etr/article/view/4732> [Accessed April 10, 2026], <https://doi.org/10.17770/etr2024vol1.7966>.
- [3] N. T. Pham, Z. Tučková and C. J. C. Jabbour, "Greening the hospitality industry: How do green HRM practices influence organizational citizenship behavior?", *Tourism Management*, Vol. 72, pp. 386–399, June 2019, [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0261517718303121?via%3Dihub> [Accessed April 10, 2026], <https://doi.org/10.1016/j.tourman.2018.12.008>.
- [4] P. Arabadzhyski, V. Vasilev, D. Sidova, "Effective Human Resource Management and Environmental Security: Protection of Human Rights and Critical Infrastructure Sustainability" in *Environment. Technology. Resources. Proceedings of the 16th International Scientific and Practical Conference*, Vol. 5, 2025, pp. 23-28, [Online]. Available: <https://archive-journals.rtu.lv/etr/article/view/5284> [Accessed April 20, 2026], <https://doi.org/10.17770/etr2025vol5.8484>.
- [5] S. Yıldırım and V. Vasilev, "The Future of Green Collar Workers: Green Transition in Employment" in *Green Transition Impacts on the Economy, Society, and Environment*, S. Yıldırım, D. Yıldırım, I. Demirtaş and V. Kandpal (Eds.), IGI Global Scientific Publishing, 2024, pp. 1-16, [Online]. Available: <https://www.igi-global.com/gateway/chapter/354189> [Accessed April 10, 2026], <https://doi.org/10.4018/979-8-3693-3985-5.ch001>.
- [6] A. B. Correia, M. Farrukh Shahzad, J. Moleiro Martins and R. Baheer, "Impact of green human resource management towards sustainable performance in the healthcare sector: Role of green innovation and risk management", *Cogent Business and Management*, Vol. 11 (1), 8 July 2024, [Online]. Available: <https://www.tandfonline.com/doi/full/10.1080/23311975.2024.2374625?scroll=top&needAccess=true#abstract> [Accessed April 10, 2026], <https://doi.org/10.1080/23311975.2024.2374625>.
- [7] P. Arabadzhyski, "Контрол на трудовите ресурси, обществените поръчки и финансите на малките и средните предприятия, осъществяващи охранителна дейност в Република България" [Control of labor resources, procurement and finance SMEs carried security in the Republic of Bulgaria/ Kontrol na trudovite resursi, obshtestvenite porachki i finansite na malkite i srednite predpriatia, osashtestvyavashti ohranitelna deynost v Republika Bulgaria], *Collection of Scientific Reports of XXVI International Scientific Conference for Young Scientists*, ISSN 1314-4669, p. 301, June 22-23, 2017. [Online]. Available: https://eprints.nbu.bg/id/eprint/4209/1/Statiq_rotated%20%281%29-2-9.pdf [Accessed April 15, 2026].
- [8] D. Stefanova, C. Popescu and V. Vasilev, "Green Transition and Human Resource Management–Sustainable Development Through Effective Management of Green Collar Workers" in *Aligning ESG Goals with the UNs Sustainable Development Goals Planning*, Malik, F.A., Kushwah, S.V., Aslam, M.S., Reyed, R.M., Haghi, A.K. (Eds.) *World Sustainability Series*. Springer, Cham, 10 January 2026, pp. 265-282 [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-032-01715-4_14 [Accessed April 10, 2026], https://doi.org/10.1007/978-3-032-01715-4_14.
- [9] Z. Grzymała and A. J. Wójcik-Czerniawska, "Building Green Skills in the Workforce as an HR Role in the Circular Economy" in *Exploring Human Resource Innovations in E-Economy*, A. Wojcik-Czerniawska (Ed.), IGI Global Scientific Publishing, 2026, pp. 121-140, [Online]. Available: <https://www.igi-global.com/gateway/chapter/406210> [Accessed April 10, 2026], <https://doi.org/10.4018/979-8-3373-4307-5.ch005>.
- [10] J. Loew, J. Mayer-Prinz, S. Spieß, M. Wagner and Y. Jiang, "Employee Green Behavior and Sustainability-Related Tensions in Teams", *Manag. Rev.*, Vol. 37 (1), 25 March 2026 [Online]. Available: <https://www.imrpess.com/journal/MRev/37/1/10.31083/MRev52> [Accessed April 10, 2026], <https://doi.org/10.31083/MRev52241>.
- [11] V. Vasilev, I. Efremovski and Z. Gigaouri, "Sustainable Human Resource Management and Development Through Innovative Approaches and Practices" in *Exploring Human Resource Innovations in E-Economy*, A. Wojcik-Czerniawska (Ed.), IGI Global Scientific Publishing, 2026, pp. 461-474, [Online]. Available: <https://www.igi-global.com/gateway/chapter/406226>

- [Accessed April 15, 2026], <https://doi.org/10.4018/979-8-3373-4307-5.ch017>.
- [12] N. Ilieva and V. Vasilev, "Green Human Resource Management and Sustainable Development: Insights from Bulgarian Organisations", *Education of Economists and Managers*, Vol. 71 (1), 8 October 2024, pp. 7–16, [Online]. Available: <https://econjournals.sgh.waw.pl/EEiM/article/view/4547> [Accessed April 15, 2026].
 - [13] J. Y. Yong, M. Y. Yusliza, T. Ramayah and, O. Fawehinmi, "Nexus between green intellectual capital and green human resource management", *Journal of Cleaner Production*, Vol. 215, 1 April 2019, pp. 364-374, [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S095965261834037X> [Accessed April 16, 2026], <https://doi.org/10.1016/j.jclepro.2018.12.306>.
 - [14] M. Ziolkowska, "Green Competencies as an Element of Sustainable Development", *Studies and Work of the Collegium of Management and Finance*, Vol. 196, 2 July 2024, pp. 161–170, [Online]. Available: <https://econjournals.sgh.waw.pl/SiP/article/view/4475> [Accessed April 16, 2026], <https://doi.org/10.33119/SiP.2024.196.12>.
 - [15] A. Matura and R. Singh, "Driving environmental stewardship: Exploring the impact of green HRM on voluntary green behaviors in higher education institutions", *Sustainable Futures*, Vol. 11, June 2026, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2666188826001231?via%3Dihub> [Accessed April 16, 2026], <https://doi.org/10.1016/j.sfr.2026.101766>.
 - [16] C. Cabral and R. L. Dhar, "Green Competencies: Insights and Recommendations from a Systematic Literature Review", *Benchmarking: An International Journal*, Vol. 28 (1), 19 January 2021, pp. 66–105, [Online]. Available: <https://www.emerald.com/bij/article-abstract/28/1/66/513475/Green-competencies-insights-and-recommendations?redirectedFrom=fulltext> [Accessed April 16, 2026], <https://doi.org/10.1108/BIJ-11-2019-0489>.
 - [17] I. Gigauri, V. Vasilev and D. Sidova, "The Role of Leadership and Corporate Social Responsibility for Sustainable Entrepreneurship: Good Practices From Georgia and Bulgaria" in *Sustainable Entrepreneurship and Family Business for Women's Empowerment*, I. Gigauri (Ed.), IGI Global Scientific Publishing, 2025, pp. 165-176, [Online]. Available: <https://www.igi-global.com/gateway/chapter/371712> [Accessed April 16, 2026], <https://doi.org/10.33119/SiP.2024.196.12>.
 - [18] Z. Afsharbakeshlo, M. Omidvar and I. Gigauri, "Green Transformational Leadership: A Systematic Literature Review and Future Research Suggestion" in *Marketing and Resource Management for Green Transitions in Economies*, J. Andrei, M. Vasić, L. Chivu and B. Kuzman (Eds.), IGI Global Scientific Publishing, 2024, pp. 47-74, [Online]. Available: <https://www.igi-global.com/gateway/chapter/352724> [Accessed April 16, 2026], <https://doi.org/10.4018/979-8-3693-3439-3.ch003>.
 - [19] KEEP, "Resilient, Sustainable and Innovative social Entrepreneurship in Central Europe", Programme 2021 - 2027 Interreg VI-B Central Europe, 9 February 2026, [Online]. Available: <https://keep.eu/projects/32824/REsiliEnt-Sustainable-and-I-EN/> [Accessed April 24, 2026].
 - [20] KEEP, "Enhancing the development of Centres of Vocational Excellence in the Danube Region by fostering competence and skill development, business-education cooperation and transnational networking", Programme 2021 - 2027 Interreg VI-B Danube, 17 December 2025, [Online]. Available: <https://keep.eu/projects/32520/Enhancing-the-development-o-EN/> [Accessed April 24, 2026].
 - [21] KEEP, "Green Skills Platform for Sustainable Employment Development", Programme 2014 - 2020 INTERREG V-A Romania - Hungary, 16 March 2023, [Online]. Available: <https://keep.eu/projects/22653/Green-Skills-Platform-for-S-EN/> [Accessed April 26, 2026].
 - [22] J. E. Thomas, D. A. Eisenberg, T. Seager and E. Fisher, "A resilience engineering approach to integrating human and socio-technical system capacities and processes for national infrastructure resilience", *Journal of Homeland Security and Emergency Management*, Vol. 16 (2), De Gruyter, 2019 [Online]. Available: <https://calhoun.nps.edu/bitstreams/8f951577-5a05-4f0e-ac0e-35a4c6388884/download> [Accessed April 21, 2026].
 - [23] C. M. Govender, "Transitioning HRM to HSM - Human Self-Management Goes beyond Traditional HR" in *Beyond Human Resources - Research Paths Towards a New Understanding of Workforce Management Within Organizations*, G. Sánchez-Gardey, F. Martín-Alcázar and N. García-Carbonell (Eds.), IntechOpen, 7 May, 2021, [Online]. Available: <https://www.intechopen.com/chapters/76658> [Accessed April 21, 2026], <https://doi.org/10.5772/intechopen.96981>.
 - [24] EU Civil Protection Knowledge Network, EET course: boosting environmental response in emergencies, 15 April 2025, [Online]. Available: <https://civil-protection-knowledge-network.europa.eu/stories/eet-course-boosting-environmental-response-emergencies> [Accessed April 21, 2026].
 - [25] K. Micklitz, G. Wong and J. Howick, "Mindfulness-based programmes to reduce stress and enhance well-being at work: a realist review", *BMJ Open*, Vol. 11 (3), 2 May 2021, [Online]. Available: <https://bmjopen.bmj.com/content/11/3/e043525> [Accessed April 21, 2026], <https://doi.org/10.1136/bmjopen-2020-043525>.
 - [26] L. Marrucci, T. Daddi and F. Iraldo, "Creating environmental performance indicators to assess corporate sustainability and reward employees", *Ecological Indicators*, Vol. 158, January 2024, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1470160X2301631X?via%3Dihub> [Accessed April 21, 2026], <https://doi.org/10.1016/j.ecolind.2023.111489>.
 - [27] J. L. Christina, R. Alamelu, M. Sathya and R. Purushothaman, "Reimagining Leadership and Organizational Culture in Digitally Native Firms: Distributed Leadership, Digital Trust, and Resilience Building in the E-Economy. in *Exploring Human Resource Innovations in E-Economy*, A. Wojcik-Czerniawska (Ed.), IGI Global Scientific Publishing, 2026, pp. 255-296. [Online]. Available: <https://www.igi-global.com/gateway/chapter/406218> [Accessed April 15, 2026], <https://doi.org/10.4018/979-8-3373-4307-5.ch010>.
 - [28] A. Singh and H. Kumar, "Green HRM: Building a Sustainable Workforce for a Greener Future" in *Exploring Human Resource Innovations in E-Economy*, A. Wojcik-Czerniawska (Ed.), IGI Global Scientific Publishing, 2026, pp. 201-216, [Online]. Available: <https://www.igi-global.com/gateway/chapter/406215> [Accessed April 15, 2026], <https://doi.org/10.4018/979-8-3373-4307-5.ch008>.
 - [29] S. I. Evangeline, "Strategic Human Resource Innovations for Sustainable Organizational Futures", in *Exploring Human Resource Innovations in E-Economy*, A. Wojcik-Czerniawska (Ed.), IGI Global Scientific Publishing, 2026, pp. 409-428, [Online]. Available: <https://www.igi-global.com/gateway/chapter/406224> [Accessed April 15, 2026], <https://doi.org/10.4018/979-8-3373-4307-5.ch015>.

Application of the Monte Carlo Method to Determine of Evacuation Parameters from Settlements

Svilen Stefanov

Logistics and Management Faculty
National Military University
Veliko Tarnovo, Bulgaria
sestefanov@abv.bg

Tihomir Yotkov

Logistics and Management Faculty
National Military University
Veliko Tarnovo, Bulgaria
tyotkov@gmail.com

Iliyan Lilov

Logistics and Management Faculty
National Military University
Veliko Tarnovo, Bulgaria
inl@abv.bg

Vanya Dimitrova

Research and Innovation Institute
National Military University
Veliko Tarnovo, Bulgaria
dimitrova_van@abv.bg

Abstract— This paper examines a potential application of the Monte Carlo method for estimating the number of people subject to evacuation during floods. Software for the simulation modelling of water disasters is utilized. The proposed method can also be applied to other crisis situations, supporting the planning of response activities and the allocation of necessary resources.

Keywords— crisis, evacuation, simulation modelling.

INTRODUCTION

Examining the Bayesian approach to risk assessment reveals that the primary methods for risk management involve reducing the probability of a hazardous event occurring and mitigating the resulting damages. When considering large-scale crises—particularly from the perspective of planning response activities by the responsible authorities—the primary practical objective is minimizing the consequences. One of the main measures in this regard is the evacuation of people from endangered areas. Evacuation, in turn, can be preventive, or it can occur during and after the onset of the crisis. Each of these types has its own specifics and characteristics, which depend on the type of crisis, the size of the endangered areas, and the propagation time of the hazard.

This paper addresses a flood-type crisis caused by a dam failure. Depending on the size of the dam, this is most often a local or regional crisis that can threaten up to several populated areas. The characteristics of the crisis indicate that the required evacuation is more likely to occur concurrently with the crisis rather than preventively. For this type of evacuation, the most critical factors are the response time and the number of endangered people who

must be evacuated. The purpose of this study is to verify the feasibility of determining precisely these factors through crisis modelling. For this purpose, the HEC-RAS software package is used [1].

CRISIS SIMULATION

For the purposes of the study, a relatively large dam with a volume of approximately 80 million m³ was selected. A map featuring a Digital Terrain Model (DTM) with a 5 x 5 m resolution was obtained from the Military Geographic Service. Files necessary for accurately determining global projections are available at <http://spatialreference.org/>. This information is provided free of charge. Furthermore, a land cover map for the entire continent with a resolution of 100 x 100 m, developed under a European Commission project, can be accessed at:

<https://ec.europa.eu/eurostat/web/gisco/geodata/reference-data/land-cover>.

This data is required to determine the hydraulic resistance (roughness) of the earth's surface within the crisis zone.

Figure 1 illustrates the terrain and dam model used for the current study. It is assumed that the event occurs at 00:00 on April 20th, and the dam wall breaches within 30 minutes, as depicted in Figure 2. In this figure, the gray area represents the dam wall, the dark gray line indicates the terrain elevation in this section, and the trapezoidal line denotes the final stage of the breach.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.71>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

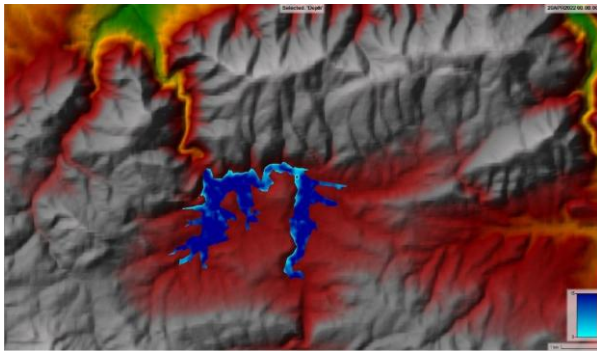


Fig. 1. Dam and terrain model.

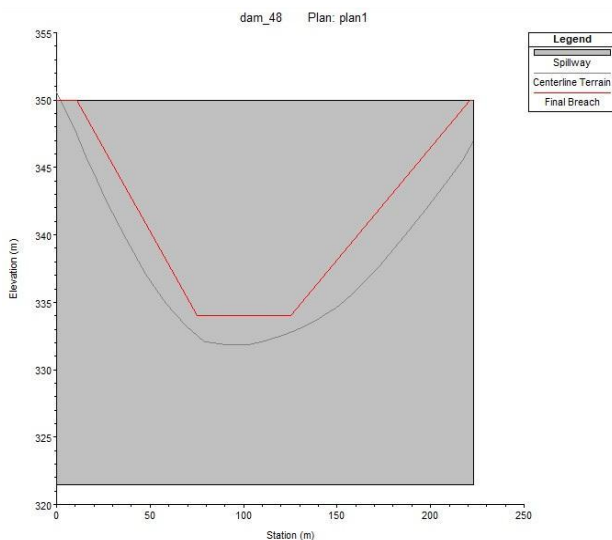


Fig. 2. Dam failure.

The HEC-RAS package utilizes a finite element approach for inundation modelling, dividing the area into cells of user-defined dimensions [2]. At a specified time step, it calculates the processes occurring within each individual cell based on the conditions of its neighbouring cells. For the purposes of this study, a cell size of 10 x 10 m and a time step of 1 second were selected. Figure 3 illustrates the inundation extent generated by the simulation within the first 24 hours following the onset of the crisis.

Along its path, the water passes through a tourist site situated at the foot of the mountain, as well as through several populated areas. The software package allows users to visualize the water level dynamics at any selected point during the simulation. Figures 4 and 5 depict the state of the tourist site before and after the flood, with an accompanying graph showing the variation of the water level over time.

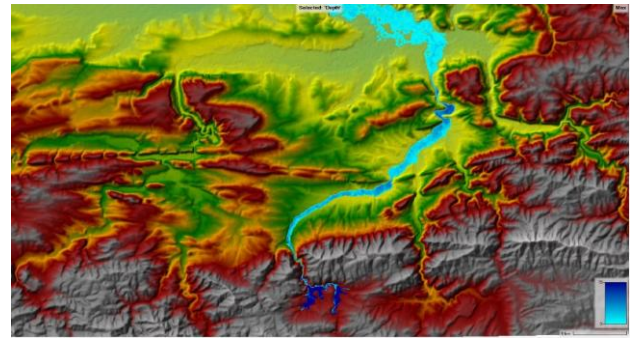


Fig. 3. Flood extent within the first 24 hours.

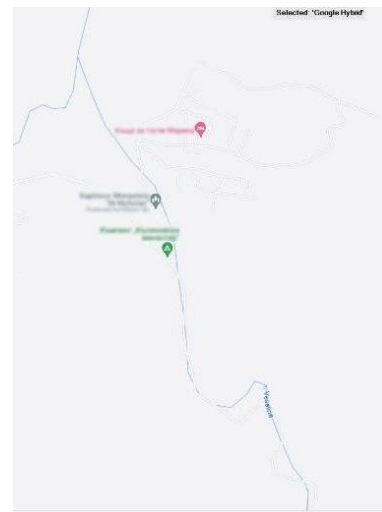


Fig. 4. Tourist site before the flood.

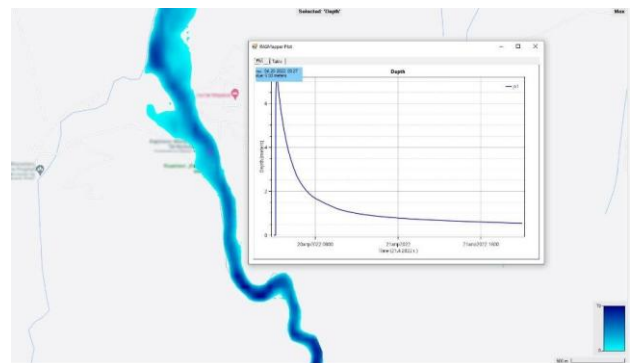


Fig. 5. Tourist site after the flood.

The graph in Figure 5 indicates that the flood wave will reach this location 27 minutes after the onset of the crisis, and its height will be approximately 7 m. On the one hand, 27 minutes is insufficient to organize an evacuation for the visitors and staff at the tourist site; on the other hand, since the inundation zone is relatively narrow, each individual could independently exit the endangered area, even on foot. However, this can only occur if they are alerted to the crisis in a timely manner. In other words, efforts here should be directed toward ensuring a timely and reliable early warning for the occupants at any time of the day or night.

To illustrate the simulation results and the possibilities for determining the factors for evacuation planning, two populated areas along the inundation path are presented. Figure 6 shows the boundaries of the populated zone (black line) for Settlement 1, as well as a graph depicting the water level dynamics.

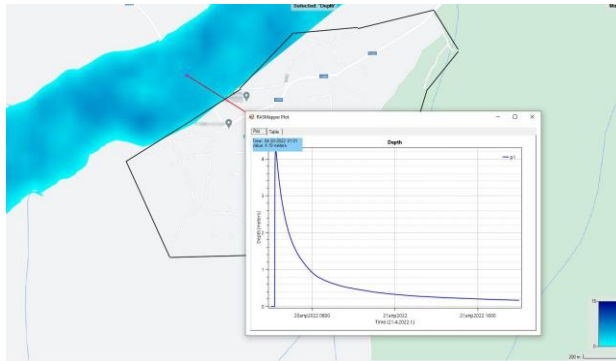


Fig. 6. Settlement 1 during the flood.

It is evident that the height of the flood wave here will be approximately 4.5 m, with an arrival time of 1 hour. Here too, the response time is short, but the residential area is only marginally affected by the flood. As with the tourist site, efforts should be directed toward alerting the people living along the riverbank and in the lower-lying areas. Local authorities and law enforcement agencies should plan to assist in the evacuation of individuals with limited mobility from the endangered areas.

Figure 7 presents the condition of Settlement 2 during the flood. Once again, the populated zone is outlined by a black line. The graph indicates that in the lower section, the water level will reach 2.5 m, which will occur 6 hours and 39 minutes after the onset of the crisis. It is evident that a significant portion of the residential area here will be endangered; however, the available response time is sufficient to prevent casualties, provided that a well-planned evacuation of the population is conducted.

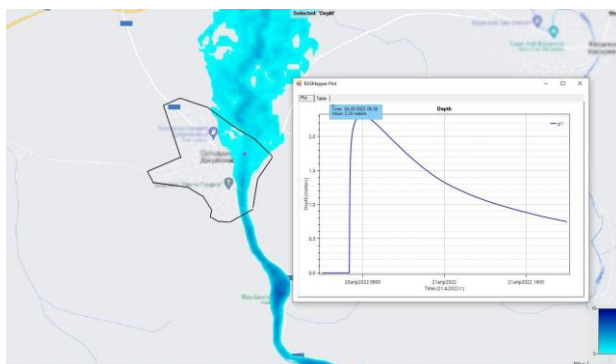


Fig. 7. Settlement 2 during the flood.

EVALUATION OF EVACUATION PARAMETERS

Information regarding the number of residents in the populated areas can be obtained from official sources (e.g., the National Statistical Institute). It remains to determine the number of people living in the endangered zone. The

settlement is of a "village" type, where people live in houses with yards. An assumption is made that the population density is relatively uniformly distributed across the area of the settlement. This allows for an approximate estimation of the number of endangered people by comparing the area of the settlement with that of the flooded section. Using modern GIS systems, the area of specific sections of the earth's surface can be determined with high precision; however, the software used for the simulation does not support these functions. Therefore, the Monte Carlo method was utilized to solve this problem [3].

In a separate image (Fig. 8), the territory of the settlement is outlined and colored yellow, while the endangered zone is colored blue.

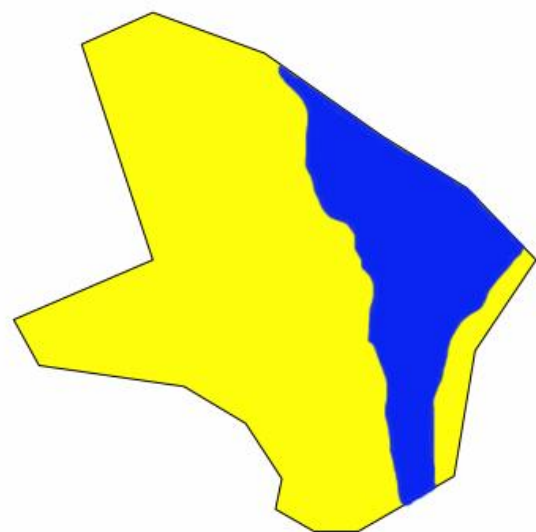


Fig. 8. Settlement area (yellow) and endangered zone (blue)

Using a script developed in Python, 1,000 points with random coordinates were generated within the image, followed by a count of the points falling into each of the colored zones. This procedure was executed 10 times. The averaged results are presented in Table 1.

TABLE 1: NUMBER OF POINTS

Zone color	Number of points
White – outside the settlement	605
Yellow – settlement	291
Blue – endangered zone	104

Figure 9 illustrates the points from one of the executions of the Monte Carlo procedure.

The total area of the settlement encompasses both the blue and yellow zones; therefore, a total of 395 points fell within this combined area. The ratio of the number of points located in the endangered zone to the total number of points in the settlement area provides an estimate of the ratio between the two areas.

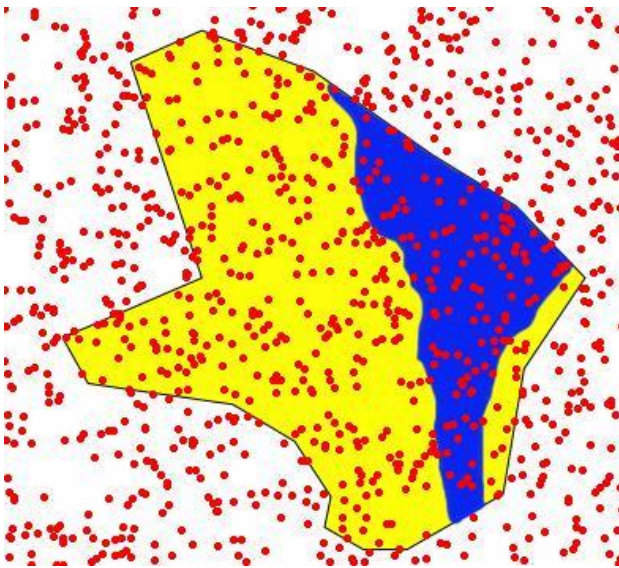


Fig. 9. Settlement area and endangered zone with 1,000 random points.

$$R = \frac{S_{flood}}{S_{village}} \cong \frac{N_{blue}}{N_{blue} + N_{yellow}}, \quad (1)$$

...where R is the ratio between the two areas;

S_{flood} – area of the endangered zone;

$S_{village}$ – area of the settlement;

N_{blue} – number of points located within the blue zone;

N_{yellow} – number of points located within the yellow zone.

Calculated according to the formula using the numerical data from Table 1, the result is $R = 0.263$, or expressed as a percentage, $R = 26.3\%$. This means that the endangered zone covers 26.3% of the settlement's total area.

Let assume that 3,000 people live here. Based on the assumption of a uniform population density distribution, we can calculate 26.3% of 3,000, which equals 789 individuals. This serves as an estimate for the number of people endangered by the flood who are potentially subject to evacuation.

The assumptions made work well for small settlements, where the housing stock predominantly consists of houses and low-rise buildings. For larger cities, a similar approach can be applied by dividing them into neighbourhoods with relatively homogeneous housing types, or in other words, with a relatively uniform population density. Furthermore, evacuation planning should account for the concentration of people in various areas of the settlement at different times of the day.

The overall results of investigating the feasibility of determining the factors necessary for the proper planning

of civilian evacuation from populated areas through crisis simulation modelling are presented in Table 2.

TABLE 2. RESULTS

Location	Total Population	Endangered Area	People to Evacuate	Available Response Time
Tourist site	500	93%	465	27 min.
Settl. 1	4500	2.5%	113	1 h.
Settl. 2	3000	26.3%	789	6 h. 39 min.

CONCLUSIONS AND FUTURE WORK

Based on the conducted research, the following conclusions can be drawn:

Modern software technologies enable the creation of models for various crisis situations with a relatively high degree of accuracy. Through these models, endangered areas can be identified, along with the threat arrival times at various settlements.

Various assumptions were utilized in the present study, which could be bypassed given precise data regarding the respective simulation elements. In this manner, the data required for planning evacuation operations can be obtained—if not to the exact individual, then at least to the correct order of magnitude. This enables the planning of necessary resources and activities tailored to both the available time and the number of people requiring evacuation.

The current study demonstrates that the simulation modelling of various types of crises can and should serve as the foundation for local governments and relevant authorities in drafting contingency plans regarding the resources and actions required for crisis response.

In this paper, the authors propose a methodology based on free software and well-established scientific methods, which can be applied to solve problems related to crisis planning and management. Despite the expected large margin of error, the obtained results can serve as a basis for planning the necessary resources, equipment, and activities required to rescue people from populated areas and regions threatened by disasters.

ACKNOWLEDGEMENTS

We would like to express our gratitude to programme “Research, Innovation and Digitalisation for Smart Transformation” 2021-2027, funded by the European Union, Project BG16RFPR002-1.014-0008 “Sustainable development of Center for Competence “Quasar” for supporting this article.

REFERENCES

- [1] Y. T. Yousif and A. N. A. Hamdan, "Flood Simulation Utilizing HEC-HMS and HEC-RAS," *Civil Engineering Journal*, vol. 12, no. 1, pp. 231-251, Jan. 2026, <https://doi.org/10.28991/CEJ-2026-012-01-013>.
- [2] H. F. Abd-Elhamid, L. A. Franzetti, M. Zelenakova, and Y. Z. Kaya, "Development of integrated hydrologic and hydrodynamic models for flood modeling in Radiša catchment at Western Slovakia using HEC-HMS and HEC-RAS," *Natural Hazards*, vol. 121, no. 18, pp. 22183-22209, Sep. 2025, <https://doi.org/10.1007/s11069-025-07683-5>.
- [3] D. Zhang, Y. Li, M. He, and X. Ke, "Accurate Calculation of the Area of Jiangnan University Based on Monte Carlo Algorithm," *International Journal of Global Economics and Management*, vol. 7, no. 1, pp. 228-234, May 2025, <https://doi.org/10.62051/ijgem.v7n1.27>.

Research on the Microelements of the Marketing Environment of Enterprises from Different Industries

Tsanko Stefanov

*Economic Theory and International Economic Relations Department
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria
c.stefanov@ts.uni-vt.bg*

Abstract—Enterprises operate within an environment that directly influences their activities. Different industries react specifically to individual elements of this environment. The main purpose of the research is to demonstrate the company's reactions to the stimuli from the environment, which has a direct impact on the activity. The subject of the research are the microelements of the marketing environment, and the object are companies from different industries in Veliko Tarnovo region.

Keywords—environment, microelements, marketing

I. INTRODUCTION

Business organizations operate under the conditions of constant influences from elements of the environment, and “company managers must consider the influence of this environment on the company's activity and take it into account when making management decisions in press” [1].

The theory highlights several elements of the environment that have a direct impact on the activities of enterprises, such as “the individual factors of this immediate environment are customers, suppliers, marketing intermediaries, contact audiences and competing firms” [2].

A similar opinion is expressed by R. Ileva, adding that “the main elements of the marketing microenvironment directly affect the state of the company's activities and contain within themselves or become conductors of the influence of the factors of the macroenvironment as well” [3].

The main dimensions of sustainable development are three interrelated elements: “economic, social, environmental. Sustainable development should not be viewed as a stagnant process, a constant of production and

consumption. On the contrary, it is dynamic, with progressive innovations - in economic, environmental and social terms, finding a wide field of application” [4].

The topic of sustainable development “with the complex of environmental, social, and economic problems is increasingly entering every sphere of public life” [5].

In general, it can be said that “in many areas of public life, research is needed into the needs of certain social groups”, as well as in various industries [6].

A. Velikova points out that “every person can make independent decisions without realizing the importance of the skills possessed for this” [7].

Thanks to their intelligence, “people have the opportunity to objectively perceive the surrounding environment and respond adequately to its factors” [8].

For N. Uzunov, “intellect is to a large extent a natural given, the ability to deeply understand tasks, problems, situations” [9].

We are now witnessing the advent of artificial intelligence, which allows for the “phased closure of activities, industries, businesses and human lives” [10].

In the article we will examine the influence of five microelements of the marketing environment: customers, suppliers, competitors, marketing intermediaries and contact audiences.

II. MATERIALS AND METHODS

For the purposes of the study, data from two business surveys conducted by the author were used. The first was conducted in the period February - May 2018 and surveyed 92 business managers from the Veliko Tarnovo region,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.42>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Bulgaria. The second survey was conducted in the period April - June 2024, in which 70 managers from the Veliko Tarnovo region were surveyed. Both surveys asked the same questions related to the company's environment, thus allowing for a temporal comparison of the results.

In both studies, companies from the Veliko Tarnovo region are divided into separate industries. The study examines representatives of the primary, secondary and tertiary sectors of the economy, such as companies from the fields of agriculture, light industry and services. This allows to highlight not only the temporal fluctuations in the opinions of company managers, but also to reveal the specifics that are characteristic of the individual sectors of the economy.

The main research method in the article is comparative analysis.

III. RESULTS AND DISCUSSION

The first and, according to many authors, the main element of the microenvironment for the company are the customers.

In this connection customer relationship management “aims to create a solid base of current and potential customers over a long period of time” [11].

The influence of customers on the activities of agricultural enterprises is presented in Table I.

TABLE I. INFLUENCE OF CUSTOMERS ON ACTIVITY OF AGRICULTURAL ENTERPRISES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	0.0	25.0
2	Low Influence	0.0	0.0
3	Medium Influence	0.0	25.0
4	Strong Influence	100.0	50.0

In 2018, managers in this industry only reported the strong influence that customers have on their business. Subsequently, the opinion changed, with most respondents still reporting a strong influence on the business from customers. Opinions also emerged about a moderate influence, and a small part of managers are not aware of the basic influence of customers on the company's business.

The influence of the “customers” factor on light industry can be seen in Table II.

TABLE II. INFLUENCE OF CUSTOMERS ON ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	0.0	33.3
2	Low Influence	6.7	0.0

№	Influence for light industry companies		
	Influence	2018	2024
3	Medium Influence	26.7	0.0
4	Strong Influence	66.7	66.7

In both studies, two-thirds of managers in light industry companies report a strong influence of customers on their activities. On the other hand, managers stop seeing a weak or moderate influence over time, but one-third of them start to think that customers do not influence the company's activities. Many authors can argue with this statement.

Table III demonstrates the influence of customers on the service sector.

TABLE III. INFLUENCE OF CUSTOMERS ON ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	6.3	0.0
2	Low Influence	0.0	0.0
3	Medium Influence	12.5	7.7
4	Strong Influence	81.2	92.3

The service sector is a sector that has seen consistency over time. To a great extent, managers in this sector understand the strong influence that customers have on their business.

Suppliers are another major element of the enterprise's microenvironment.

Table IV shows the influence of suppliers on the activities of agricultural companies.

TABLE IV. INFLUENCE OF SUPPLIERS ON ACTIVITY OF AGRICULTURAL ENTERPRISES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	33.3	0.0
2	Low Influence	0.0	0.0
3	Medium Influence	0.0	100.0
4	Strong Influence	66.7	0.0

It is notable that all managers in the agricultural sector are beginning to consider the influence of suppliers on their activities. However, over time, managers are fully beginning to accept that this influence is moderate, while in 2018 most reported a strong influence. It is possible that the COVID-19 crisis has led to certain business decisions that reduce the business's dependence on suppliers to some extent, without completely eliminating it, such as

maintaining more stocks of necessary raw materials and supplies, including more protective clauses in contracts with suppliers, and others.

How suppliers, as a microelement of the environment, influence the activities of light industry companies is presented in Table V.

TABLE V. INFLUENCE OF SUPPLIERS ON ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	6.7	0.0
2	Low Influence	13.3	11.1
3	Medium Influence	40.0	0.0
4	Strong Influence	40.0	88.9

In the light industry, there is an increase in the impact of suppliers on operations. To a very large extent, managers in the industry report a strong impact from suppliers.

The following table (Table VI) demonstrates the influence of suppliers on the activities of service companies.

TABLE VI. INFLUENCE OF SUPPLIERS ON ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	25.0	7.7
2	Low Influence	0.0	7.7
3	Medium Influence	31.2	38.5
4	Strong Influence	37.5	46.2

In the services sector, no serious changes have been observed over time. There is a slight increase in the number of managers who believe that suppliers have a moderate and strong impact on the activities of the enterprise, and it is positive that there is a decrease in the number of managers who think that suppliers have no impact on the activities of their enterprises.

Competitors are considered by most authors as an element of the microenvironment of firms.

Table VII presents the influence of competitors on the overall activities of agricultural companies.

TABLE VII. INFLUENCE OF COMPETITORS ON ACTIVITY OF AGRICULTURAL ENTERPRISES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	0.0	50.0
2	Low Influence	0.0	25.0
3	Medium Influence	33.3	0.0
4	Strong Influence	66.7	25.0

There is a significant increase in the number of managers in the agricultural sector who do not think that competitors have an impact on the activities of their enterprises. Opinions about a weak impact of competitors are emerging, at the expense of the moderate and strong impact that were reported in the first study.

How competitors influence light industry companies is presented in the following table (Table VIII).

TABLE VIII. INFLUENCE OF COMPETITORS ON ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	13.3	11.1
2	Low Influence	33.3	0.0
3	Medium Influence	26.7	0.0
4	Strong Influence	26.7	88.9

Managers of light industry enterprises think in the opposite direction to managers from the agricultural sector. They are increasingly aware of the strong influence that competitors have on the company's activities.

The influence of competitors on the activities of the service sector is demonstrated below (Table IX).

TABLE IX. INFLUENCE OF COMPETITORS ON ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	6.3	7.7
2	Low Influence	6.3	23.1
3	Medium Influence	31.2	30.8
4	Strong Influence	37.5	38.5

In the services sector, there is stability over time in the opinion about the impact of competitors on company

activities. However, the majority of managers in the sector report a moderate or strong impact of this microfactor.

The extent to which marketing intermediaries influence the activities of enterprises in various industries as microelements of the surrounding environment will be discussed in the following lines.

The influence of marketing intermediaries on company activities in the agricultural sector is presented in Table X.

TABLE X. INFLUENCE OF MARKETING INTERMEDIARIES ON ACTIVITY OF AGRICULTURAL ENTERPRISES

№	Influence for agricultural enterprises		
	<i>Influence</i>	2018	2024
1	Without Influence	0.0	50.0
2	Low Influence	33.3	25.0
3	Medium Influence	66.7	25.0
4	Strong Influence	0.0	0.0

Managers of agricultural enterprises have never perceived marketing intermediaries as a factor with a strong impact on the company's activities. However, over time, those who think that the impact is moderate are also decreasing. In 2024, half of the managers in this sector believe that marketing intermediaries do not affect the company's activities.

Table XI presents the opinions of light industry managers regarding the influence of marketing intermediaries on the activities of their enterprises.

TABLE XI. INFLUENCE OF MARKETING INTERMEDIARIES ON ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	<i>Influence</i>	2018	2024
1	Without Influence	33.3	11.1
2	Low Influence	26.7	44.4
3	Medium Influence	33.0	33.3
4	Strong Influence	6.7	11.1

No serious changes are observed in the light industry, but the position of weak influence on the part of marketing intermediaries as a microfactor is strengthening.

How marketing intermediaries influence a company's activities in the service sector is presented in Table XII.

TABLE XII. INFLUENCE OF MARKETING INTERMEDIARIES ON ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	<i>Influence</i>	2018	2024
1	Without Influence	50.0	30.8

№	Influence for service sector		
	<i>Influence</i>	2018	2024
2	Low Influence	18.7	7.7
3	Medium Influence	18.7	30.8
4	Strong Influence	6.3	30.8

Only in the services sector is there a more serious increase in managers who report moderate and strong influence on the company's activities from marketing intermediaries.

Contact audiences, as a full-fledged microelement of the environment for organizations, directly impact their activities.

Table XIII demonstrates the influence, according to managers, of contact audiences on the activities of companies in the agricultural sector.

TABLE XIII. INFLUENCE OF CONTACT AUDIENCES ON ACTIVITY OF AGRICULTURAL ENTERPRISES

№	Influence for agricultural enterprises		
	<i>Influence</i>	2018	2024
1	Without Influence	33.3	25.0
2	Low Influence	33.3	0.0
3	Medium Influence	0.0	75.0
4	Strong Influence	33.3	0.0

Regarding contact audiences in the agricultural sector, there is a significant shift towards the opinion of a moderate impact on company activities.

How contact audiences influence the activities of light industry companies is presented below . (Table XIV).

TABLE XIV. INFLUENCE OF CONTACT AUDIENCES ON ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	<i>Influence</i>	2018	2024
1	Without Influence	53.3	22.2
2	Low Influence	20.0	44.4
3	Medium Influence	26.7	33.3
4	Strong Influence	0.0	0.0

In the light industry sector, contact audiences are not traditionally viewed as having a strong impact. There is a shift towards a weak impact, as in the first period of the study, half of the managers in the sector did not report an impact of this microfactor on the activities of the enterprises.

The influence of contact audiences on the activities of service companies is presented in Table XV.

TABLE XV. INFLUENCE OF CONTACT AUDIENCES ON ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	56.3	53.8
2	Low Influence	25.0	7.7
3	Medium Influence	12.5	15.4
4	Strong Influence	6.3	23.1

In service companies, most managers do not report the influence of contact audiences on the business.

The environment is dynamic and company managers must take this into account. With the development of digitalization in most business activities and the use of CRM systems, social networks, the strengthening of e-commerce and the introduction of artificial intelligence, the perception of the microenvironment by company managers is changing.

These innovations have an impact on the structure of the microenvironment and its individual elements. The changed conditions can provide advantages, but can also create obstacles to company activities. This depends on the reaction of their managers.

IV. CONCLUSIONS

The results presented in the article show interesting trends. First of all, it should be noted that, consistently, customers have the greatest influence on a company's activities, with their influence being most pronounced in service companies.

Competing companies also have a serious impact, especially in the light industry sector.

There are interesting fluctuations among suppliers, but overall they are also among the microfactors with a significant impact on business.

The least considered is the influence of marketing intermediaries and contact audiences, which in most cases either have a slight impact or their impact on business activity is not taken into account.

In future research, it will be interesting to examine how the use of artificial intelligence, big data, and cloud technologies changes the way that companies interact with their customers and suppliers.

It is also appropriate in future research and analysis to compare the data obtained for the Veliko Tarnovo region with other regional data or data at the national or European level.

REFERENCES

- [1] T. Stefanov, Market strategy and building company competitiveness in Veliko Tarnovo region. Veliko Tarnovo: Faber, 2018.
- [2] T. Stefanov, Marketing solutions for modern business. Veliko Tarnovo: Faber, 2020.
- [3] R. Ileva, Marketing. Veliko Tarnovo: Abagar Publishing House, 2008.
- [4] P. Penchev and I. Pencheva, Basics of Management. Veliko Tarnovo: Abagar Publishing House, 2002.
- [5] V. Tsonkova, Sovereign Sustainable Bond Market – Positioning and Effects, Proceedings of the 15th International Scientific and Practical Conference "Environment. Technology. Resources", vol. I, pp. 388-392, Rezekne, Latvia, 2024.
- [6] A. Velikova, Planning and development of social services in a regional aspect, Proceedings of the Scientific Conference "Logistics and Social Systems", Februari 25-27, 2021, Veliko Tarnovo: Publishing complex of the National Military University "Vasil Levski", pp. 594-599, 2021.
- [7] A. Velikova, Training for the acquisition of skills for persons with intellectual disabilities as a form of empowerment, Proceedings of the Scientific and Practical Conference "Development of the Bulgarian and European Economy - Challenges and Opportunities", May 27-28, 2022, Veliko Tarnovo: University publishing house, 2022.
- [8] I. Stoykov, General psychopathology. Veliko Tarnovo: IVIS, 2009.
- [9] N. Uzunov, Basics of psychology. Sofia: Siela Soft and Publishing AD, 2008.
- [10] S. Lakova, Perspectives for the development of political brands, Proceedings of the Annual University Scientific Conference June 8 - 9, 2023, Veliko Tarnovo: Publishing Complex of the Vasil Levski National Military University, vol. 12, 2023.
- [11] T. Stefanov, "Management Policy of Company Key Customers", in "Economic Studies", vol. 27 (6), pp. 136 – 140, Sofia, 2018.

Research on the Macro Elements of the Marketing Environment of Companies by Industry

Tsanko Stefanov

Economic Theory and International Economic Relations Department
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria
c.stefanov@ts.uni-vt.bg

Abstract—Companies operate in the conditions of environmental factors, some of which do not directly affect their activities, but through indirect influence. The subject of the development are the macro factors of the companies' environment, and the object is the business in the Veliko Tarnovo region. The main goal is to present the reactions to changes in the macro factors of the environment and how this can affect the company's competitiveness. The research objective is to compare the temporal influences of individual factors on company activity. The main research method is comparative analysis. The main result of the study is the identification of the specifics of influences in different industries.

Keywords—environment, industry, macro factors, marketing

I. INTRODUCTION

Business organizations do not operate in isolation. They are under the conditions of constant influences from elements of the environment.

Companies are surrounded by factors that have an impact on them. This environment is not static and “its elements undergo continuous changes, which are often unexpected for companies” [1].

Therefore, in order to be more adequate to the impacts “it is important for the company to build a specialized communication system” [2].

This communication system receives information to the organization and sends information out of it. In this regard, S. Lakova notes that “the originality of the communicated message is the most important prerequisite for the formation of trust and even for choice, through a conscious decision” [3].

The first direction of environmental factors directly affects companies and is part of the microenvironment.

Considering this environment “institutions are forced to look for new forms of interaction with contractors and users of their services” [4].

The second direction “encompasses factors that first affect the elements of the organization's microenvironment and then their influence is transmitted to the company itself” [5].

As R. Ileva notes “along with the rapidly changing global picture, the company must monitor the macroenvironmental factors, which are numerous, but can be divided into six main groups: demographic, economic, natural, technological, political and cultural” [6].

Sustainable development is “an objective necessity for the future, but effective action should be taken now to implement it” [7].

The topic of sustainable development “with the complex of environmental, social, and economic problems is increasingly entering every sphere of public life” [8].

In general, it can be said that “in many areas of public life, research is needed into the needs of certain social groups”, as well as in various industries [9].

The article will examine six macro elements of the marketing environment: demographic environment, economic environment, natural environment, political environment, technological environment, and cultural environment.

The research objective is to compare the temporal influences of individual factors on company activity and the main research method is comparative analysis. Three main industries in the territory of the Veliko Tarnovo region are being studied, as part of the three levels of the economy.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.43>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

II. MATERIALS AND METHODS

The article includes results from two studies on business organizations conducted by the author in the Veliko Tarnovo region, Bulgaria. The first was carried out in the period February - May 2018 and 92 business leaders from the region were surveyed. The second survey was conducted between April and June 2024 and included 70 business managers.

In both surveys, invitations were sent to the same respondents. The number of respondents was different in the two surveys due to the different proportion of managers who agreed to participate in the survey.

This represents a limitation of the study, which may, to a small extent, fail to take into account the opinions of managers from the second survey.

Also regarding the limitations, the study of macroenvironmental factors in Bulgaria is not popular and it is difficult to compare the results of this study with other similar studies in order to make the results comparable.

Both surveys asked questions related to the environment as part of a larger study of the management and marketing activities of enterprises.

The questionnaire includes over 30 questions regarding the management and marketing activities of the companies, which are mainly closed with pre-set answers or have a rating scale.

Evidence of empirical data regarding the influence of the macroenvironment on the activities of companies in the region under consideration is available in the author's cited monograph.

In both studies, stratification was made by different industries. Enterprises were divided into sectors: agriculture, heavy industry, light industry, construction, transport, trade, tourism and services.

The article will consider companies from agriculture, light industry and services, as representatives of the primary, secondary and tertiary sectors of the economy.

The main research method used (comparative analysis) allows for comparing the results obtained over time and revealing key specifics in different industries.

The study clearly links to the PESTEL model, but there are some differences, as the social environment is represented by demographic factors, cultural factors are identified as a separate element, and legal factors are combined with political ones.

As part of future research, it is appropriate to examine the results of the PESTEL analysis through the prism of a SWOT analysis.

III. RESULTS AND DISCUSSION

The cited authors and leading writers in the field of marketing are unanimous about the significant impact of the macroenvironment on business operations.

Whether entirely indirectly or with insights into certain direct impacts on organizations, they examine this environment in terms of distinct, separable elements.

The same applies to the presentation of the elements below.

The first macroelement of the environment is the demographic environment.

The influence of demographic environment on the activities of agricultural companies is presented in Table I.

TABLE I. INFLUENCE OF DEMOGRAPHIC ENVIRONMENT ON THE ACTIVITY OF AGRICULTURAL COMPANIES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	0.0	25.0
2	Low Influence	0.0	25.0
3	Medium Influence	33.3	25.0
4	Strong Influence	66.7	25.0

The demographic environment is having a decreasing impact on the activities of agricultural enterprises.

The influence of the demographic environment on the light industry sector can be traced in Table II.

TABLE II. INFLUENCE OF DEMOGRAPHIC ENVIRONMENT ON THE ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	20.0	0.0
2	Low Influence	33.3	22.2
3	Medium Influence	26.7	55.6
4	Strong Influence	20.0	22.2

In the light industry sector, there is an increase in managers who believe that the demographic environment has a moderate impact on business. It is positive that over time there are no managers who do not take into account the impact of this environment on company activities.

Table III demonstrates the impact of the demographic environment on the services sector.

TABLE III. INFLUENCE OF DEMOGRAPHIC ENVIRONMENT ON THE ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	12.5	7.7
2	Low Influence	18.7	23.1

№	Influence for service sector		
	Influence	2018	2024
3	Medium Influence	43.7	23.1
4	Strong Influence	18.7	46.2

In service companies, there is a certain growth in managers who report a strong impact of the demographic environment.

The demographic environment is a projection of the organization's market. To report the decline in the influence of this environment is most likely indicative of the weak theoretical knowledge of managers in this industry and specifically in agriculture.

A major macro factor in the business environment is the economic environment.

Table IV shows the impact of the economic environment on the activities of agricultural companies.

TABLE IV. INFLUENCE OF ECONOMIC ENVIRONMENT ON THE ACTIVITY OF AGRICULTURAL COMPANIES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	0.0	0.0
2	Low Influence	0.0	25.0
3	Medium Influence	33.3	25.0
4	Strong Influence	66.7	50.0

In the agricultural sector, there is a slight decrease in managers reporting a moderate and strong impact of the economic environment on the business.

The influence of the economic environment on the activities of light industry companies is presented in Table V.

TABLE V. INFLUENCE OF ECONOMIC ENVIRONMENT ON THE ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	6.7	0.0
2	Low Influence	20.0	22.2
3	Medium Influence	33.3	55.6
4	Strong Influence	40.0	22.2

Light industry managers are increasingly beginning to take into account the moderate impact of the economic environment on their activities.

Table VI demonstrates the impact of the economic environment on the activities of service companies.

TABLE VI. INFLUENCE OF ECONOMIC ENVIRONMENT ON THE ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	0.0	15.4
2	Low Influence	0.0	7.7
3	Medium Influence	31.2	7.7
4	Strong Influence	62.5	69.2

Among companies in the service sector, the leading opinion is that the economic environment has a strong impact on company activities.

Managers in the service sector are most likely to adequately account for the economic impact on their business. Managers in agriculture are most likely to neglect monitoring the economic environment.

An important macroelement of the company's environment is the natural environment.

It includes natural resources that are “extraordinarily diverse in quantity, variability, renewability and reusability” [10].

Table VII presents the impact of the natural environment on the activities of agricultural companies.

TABLE VII. INFLUENCE OF NATURAL ENVIRONMENT ON THE ACTIVITY OF AGRICULTURAL COMPANIES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	0.0	0.0
2	Low Influence	0.0	0.0
3	Medium Influence	0.0	0.0
4	Strong Influence	100.0	100.0

All managers in the agricultural sector recognize the strong impact of the natural environment on their activities, as their activities are most directly related to nature.

What is the influence of the natural environment on light industry is clarified by the following table (Table VIII).

TABLE VIII. INFLUENCE OF NATURAL ENVIRONMENT ON THE ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	40.0	55.6
2	Low Influence	46.7	33.3
3	Medium Influence	6.7	11.1
4	Strong Influence	6.7	0.0

To a large extent, light industry managers do not consider the impact of their activities on the natural environment, but they must consider that their raw materials depend on this environment.

The impact of the natural environment as a macro factor on the activity of the service sector is demonstrated by Table IX.

TABLE IX. INFLUENCE OF NATURAL ENVIRONMENT ON THE ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	43.7	41.7
2	Low Influence	18.7	16.7
3	Medium Influence	6.3	41.7
4	Strong Influence	12.5	0.0

Many managers in the service sector also do not consider the influence of the natural environment, but over time there has been an increase in those who consider the moderate impact of this environment on their activities.

It is quite logical that the natural environment has a very strong impact on the agricultural sector, but its impact is not limited to this industry. Managers in the secondary and tertiary sectors of the economy must also take these influences into account, given their connection with the factors of production, especially in light industry.

The next macro factor of the environment for organizations is the political environment.

The influence of the political environment on company activity in the agricultural sector is presented in Table X.

TABLE X. INFLUENCE OF POLITICAL ENVIRONMENT ON THE ACTIVITY OF AGRICULTURAL COMPANIES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	0.0	0.0
2	Low Influence	33.3	25.0
3	Medium Influence	66.7	50.0

№	Influence for agricultural enterprises		
	Influence	2018	2024
4	Strong Influence	0.0	25.0

The political environment has the greatest moderate impact on the activities of agricultural enterprises. The minimum purchase prices set by the government for their products are very important for them.

Table XI presents the opinions of light industry managers on the impact of the political environment as a factor of the macro environment.

TABLE XI. INFLUENCE OF POLITICAL ENVIRONMENT ON THE ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	33.3	55.6
2	Low Influence	33.3	0.0
3	Medium Influence	33.3	22.2
4	Strong Influence	0.0	22.2

To a significant extent, light industry managers believe that the political environment does not affect their business, but they should take into account changes in special laws related to their activities.

The influence of the political environment on company activity in the service sector is presented in Table XII.

TABLE XII. INFLUENCE OF POLITICAL ENVIRONMENT ON THE ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	25.0	61.5
2	Low Influence	31.2	15.4
3	Medium Influence	25.0	0.0
4	Strong Influence	6.3	23.1

In the service sector, even more so than in light industry, serious attention is not paid to the political environment. Managers need to do better monitoring of legislative changes and the government's views on the direction of economic development.

In all three sectors of the economy, insufficient attention is paid to the influence of political and legal factors on the activities of the organization. Given the political instability in Bulgaria, business managers need to conduct a more in-depth analysis of the political environment, which has a strong impact on both the economic and demographic elements.

The technological environment is a macro element of the company's environment, together with the elements discussed so far.

Table XIII presents the influence of the technological environment on the activities of companies in the agricultural sector.

TABLE XIII. INFLUENCE OF TECHNOLOGICAL ENVIRONMENT ON THE ACTIVITY OF AGRICULTURAL COMPANIES

№	Influence for agricultural enterprises		
	Influence	2018	2024
1	Without Influence	0.0	0.0
2	Low Influence	0.0	0.0
3	Medium Influence	33.3	75.0
4	Strong Influence	66.7	25.0

Managers in the agricultural sector take technological change seriously as a factor affecting their operations. All in this sector report either a moderate or strong impact of the macroelement.

How the technological environment affects the light industry sector can be seen from Table XIV.

TABLE XIV. INFLUENCE OF TECHNOLOGICAL ENVIRONMENT ON THE ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for light industry companies		
	Influence	2018	2024
1	Without Influence	6.7	0.0
2	Low Influence	33.3	55.6
3	Medium Influence	6.7	33.3
4	Strong Influence	53.3	11.1

Interesting results are obtained for the light industry sector. There is an atypical increase in those managers who believe that the technological impact on the activity is weak. They should think strategically in the long term, because their outdated productions cannot bring them competitive advantages in the future.

The influence of the technological environment as a macro-element of the environment on the activity of service companies is presented in Table XV.

TABLE XV. INFLUENCE OF TECHNOLOGICAL ENVIRONMENT ON THE ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	18.7	61.5

№	Influence for service sector		
	Influence	2018	2024
2	Low Influence	18.7	0.0
3	Medium Influence	18.7	7.7
4	Strong Influence	37.5	30.8

To a very large extent, service company managers do not consider the technological environment as a serious influencing factor. This should be changed so that they do not seriously reduce their company competitiveness.

Only managers in the primary sector recognize the great importance of new technologies for the development of their activities. In the other sectors of the region, low-tech activity is observed, but investments in new technologies should be made to increase company competitiveness.

The last macrofactor of the organizational environment is the cultural environment.

Table XVI shows the influence of the cultural environment on the activities of agricultural companies.

TABLE XVI. INFLUENCE OF CULTURAL ENVIRONMENT ON THE ACTIVITY OF AGRICULTURAL COMPANIES

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	66.7	25.0
2	Low Influence	33.3	75.0
3	Medium Influence	0.0	0.0
4	Strong Influence	0.0	0.0

In agriculture sector, the cultural factor is either not taken into account or is taken into account with little impact on business.

The influence of the cultural environment on the light industrial sector can be seen in Table XVII.

TABLE XVII. INFLUENCE OF CULTURAL ENVIRONMENT ON THE ACTIVITY OF LIGHT INDUSTRY COMPANIES

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	33.3	22.2
2	Low Influence	40.0	22.2
3	Medium Influence	26.7	55.6
4	Strong Influence	0.0	0.0

In the light industry sector, there has been a slight increase in those managers who report a moderate impact of the cultural environment on their activities.

The impact of the cultural environment as a macro factor is presented in Table XVIII.

TABLE XVIII. INFLUENCE OF CULTURAL ENVIRONMENT ON THE ACTIVITY OF ENTERPRISES FROM THE SERVICE SECTOR

№	Influence for service sector		
	Influence	2018	2024
1	Without Influence	37.5	30.8
2	Low Influence	25.0	23.1
3	Medium Influence	18.7	23.1
4	Strong Influence	6.3	23.1

In the service sector, the influence of the cultural environment is taken into account to a greater extent, with a slight increase in the number of managers who report a moderate or strong impact on their business.

The cultural factor is considered to be the most important factor in the development or limitation of a company's activity in the service sector.

The influence of the cultural element increases consistently at different levels of the economy - from a weak influence in the primary sector, to a moderate influence in the secondary sector, and to the most significant influence in the tertiary sector of the economy.

IV. CONCLUSIONS

Based on the results obtained from the two studies, some trends emerged.

The demographic environment is not sufficiently considered by companies in all three industries as a factor that has a strong impact on the activity. Considering that the market consists of people, it is important to pay more attention when conducting an analysis from a demographic perspective and to improve the theoretical knowledge of managers, especially in the primary sector of the economy.

The economic environment is considered a factor with a significant impact on the activities of companies in all three sectors but this is insufficiently monitored in the primary sector of the economy.

Quite logically, agricultural enterprises take into account the strong influence of the natural environment on company activities to the greatest extent. The impossibility of production without the necessary factors of production makes it mandatory to monitor and analyze the natural environment at all levels of the economy.

Service companies and light industry enterprises largely do not take into account the impact of political macro factors on the company's operations. The legal framework, the political climate, and their impact on other elements of the business environment should be the focus of corporate managers' analysis.

The technological environment is considered to be the most influential factor for the activities of agricultural enterprises. In other sectors, more attention needs to be paid to technological factors and managers should invest in new technologies to increase the efficiency of company operations.

The influence of the cultural environment is more noticeable in the service sector and light industry, while for agricultural companies this influence is not significant.

The results of the study of the macro environment are useful for managers from the considered spheres of activity, who can base themselves on them to increase their company's competitiveness. The results are practically applicable to other industries from the three levels of the economy of the region, and in the future, when conducting a national study, they can be the basis for application at the national level.

REFERENCES

- [1] T. Stefanov, Market strategy and building company competitiveness in Veliko Tarnovo region. Veliko Tarnovo: Faber, 2018.
- [2] T. Stefanov, Management Policy of Company Key Customers", "Economic Studies", vol. 27 (6), pp. 136 – 140, Sofia: Economic Research Institute at the Bulgarian Academy of Sciences, 2018.
- [3] S. Lakova, Aspects of pre-election communication of the political party Vazrazhdane, Development of the Bulgarian and European economy - challenges and opportunities, May 26, 2023, Veliko Tarnovo: University Publishing House, Veliko Tarnovo, vol. 7, 2023.
- [4] S. Lakova, Mechanism for supporting the activities of the non-profit sector in municipalities, Proceedings of the Annual University Scientific Conference May 27 - 28, 2021, Veliko Tarnovo: Vasil Levski National University Publishing Complex, vol. 8, 2021.
- [5] T. Stefanov, Marketing solutions for modern business. Veliko Tarnovo: Faber, 2020.
- [6] R. Ileva, Marketing, Veliko Tarnovo: Abagar, 2008.
- [7] P. Penchev and I. Pencheva, Basics of Management. Veliko Tarnovo: Abagar Publishing House, 2002.
- [8] V. Tsonkova, Sovereign Sustainable Bond Market – Positioning and Effects, Proceedings of the 15th International Scientific and Practical Conference "Environment. Technology. Resources", vol. I, pp. 388-392, Rezekne, Latvia, 2024.
- [9] A. Velikova, Planning and development of social services in a regional aspect, Proceedings of the Scientific Conference "Logistics and Social Systems", Februari 25-27, 2021, pp. 594-599, Veliko Tarnovo, Bulgaria. Veliko Tarnovo: Publishing complex of the National Military University "Vasil Levski", 2021.
- [10] O. Owen, Conservation of Natural Resources, Part Two, Sofia: Zemizdat, 1989.

Operational Art and Cognitive Warfare

Milko Stefanov

Rakovski National Defense College
Sofia, Bulgaria
m.j.stefanov@rndc.bg

Abstract— The report examines the transformation of operational art under the influence of cognitive warfare. The main focus is on the strategic asymmetry between the leading global military doctrines. Through a systematic analysis, differences in approaches are revealed – NATO’s reactive-defensive model aimed at societal resilience; the US’s proactive model striving for cognitive dominance; Russia’s offensive reflexive management and China’s intellimentized warfare. The results of the study prove that the cognitive dimension is becoming a critical factor for success in multi-domain operations, where victory is defined by breaking the enemy’s will and paralyzing his decision-making processes. Guidelines are proposed for integrating cognitive effects into operational design and developing new metrics for effectiveness.

Keywords— *cognitive warfare, operational art, cognitive superiority, doctrinal asymmetry.*

I. INTRODUCTION

The nature of war is undergoing a transformation. Conflicts are no longer confined to the traditional domains of land, air, and sea, but are being transferred to the intangible spaces of information and human consciousness. In this new reality, the human mind becomes the primary battlefield – both target and weapon. This change questions and reshapes the very foundations of military thought, elevating cognitive warfare from a tactical tool to a strategic force transforming operational art.

Given the topicality and discursive nature of the problem posed for consideration, the main goal of the publication is to explore the integration of cognitive warfare into contemporary operational art, analyzing the strategic asymmetry between Western (NATO and the USA) and Eastern (Russia and China) military doctrines. In the context of the research objective, the evolution from psychological operations to neurologically based influence is traced and the research question is sought to answer how differences in national philosophies – from building democratic resilience to offensive reflexive governance and intellimentized warfare – determine the dynamics of

contemporary geopolitical competition. Through the conducted analysis and synthesis, the aim is to define how the cognitive dimension is reformulating the processes of operational planning, decision-making and achieving strategic superiority in the era of digital hyper-connectivity and artificial intelligence.

II. MATERIALS AND METHODS

To achieve the research objectives, official military doctrines and conceptual documents were analyzed. Publications of leading researchers in the field of cognitive warfare such as Backes & Swab, Miller, Claverie & du Cluzel and others were used. Data from specialized centers of excellence (NATO ACT, StratCom CoE) and studies of Eastern military models were included.

For the needs of the publication, a systematic analysis was applied to reveal the transformation of operational art under the influence of cognitive factors and to define cognitive warfare as a multi-layered phenomenon. A comparative analysis was used to identify the strategic asymmetry between Western and Eastern military doctrines. A new definition of cognitive warfare was derived through the synthesis method, integrating technological, informational and psychological aspects. Conceptual modeling was used in examining the processes of operational planning and operational design, in order to identify non-physical centers of gravity and new metrics for effectiveness.

III. RESULTS AND DISCUSSION

A. Defining cognitive warfare

Central to cognitive warfare theory is the concept of the human mind as a contested territory or battlefield. This reframes conflict from a physical contest to one in which perception and decision-making are the primary objectives. In defining cognitive warfare, the authors agree on the idea that it is not simply a technological process, but one that aims to change the human condition. The publications of Backes and Swab [1], Hung and Hung [2] and NATO ACT [3] emphasize that the goal is not only to change thinking,

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.45>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

but to lead to a specific action or inaction that serves the interests of the attacker. In addition, both the analysis of Miller [4] and the NATO ACT document recognize that, unlike cyberwarfare, which attacks software, or kinetic warfare, which attacks physical objects, cognitive warfare targets mental states, decision-making and perceptions. Tashev [5] and Hung and Hung recognize that cognitive warfare is related to information, but goes further – it is not about the transfer of data, but about the effect that this data causes in the brain, i.e. achieving the cognitive effect. A wide range of means is used to achieve this – from technology and media to social environment and legal norms.

The differences in definitions stem mainly from where the authors position cognitive warfare in the hierarchy of military conflicts and what methods they emphasize. Hung and Hung, Tashev and Ninov, Borisova and Dragova [6] do not consider cognitive warfare as a completely separate phenomenon. For Hung and Hung, Ninov, Borisova and Dragova, it is a subset of hybrid warfare. For Tashev, it is simply an aspect of information warfare or part of the overall portfolio of national power. Miller, Backes and Swab define it as a separate field with specific objectives, such as response management and psychological harm, distinct from cyber or information warfare. In terms of operational threshold and scope, Miller strictly positions cognitive warfare as an activity that operates below the threshold of conventional conflict to subtly undermine institutions. Unlike Miller, the NATO definitions and Chinese concepts allow for cognitive warfare to be conducted in both peacetime and wartime, and may also include kinetic actions to achieve psychological effect. The authors also emphasize different methods depending on national doctrines. In the Chinese model, Hung and Hung emphasize the manipulation of environmental stimuli and the connection with the three wars – psychological, public opinion and legal. In the Russian model, Tashev and Hansen [7] point to information operations as part of a massive, state-led approach to influence. The Western/NATO model focuses on technology, the protection of democratic institutions, individual psychology and the resilience of society. Conceptually, it is important to distinguish cognitive from information warfare and psychological operations. While in information warfare the processes are related to the control and flow of information, in psychological operations (PSYOPS) the object of influence is emotions and attitudes, often through messages. Cognitive warfare is aimed at the very mechanisms of cognition – how the brain processes information to form understanding and make decisions [8]. The main focus is on changing how people think, not just what they think.

From the analysis made, for the needs of the report, the following definition can be formulated:

"Cognitive warfare is the integration of technological, informational, and psychological capabilities to manipulate perceptions and behavior, with the aim of disorienting the adversary's decision-making processes and achieving strategic effects comparable to or superior to those of kinetic force."

B. Doctrinal and conceptual foundations of cognitive warfare

a) NATO's approach – collective defense in the cognitive domain.

NATO's Strategic Communications (StratCom) doctrine provides the institutional context for the Alliance's approach to the information environment. StratCom is defined as the coordinated use of public diplomacy, public relations, military public relations, information operations and PSYOPS to achieve Alliance objectives [9]. Events such as the conflict in Afghanistan and the Russian invasion of Ukraine in 2014 have exposed the limitations of this traditional approach. The main focus of NATO's adaptation has been on developing a specific concept of cognitive warfare, guided by NATO ACT. It states that adversaries actively target the cognitive dimension to undermine public cohesion and political will [3]. NATO's working definition is: "activities conducted in concert with other instruments of power to influence attitudes and behaviour by influencing, protecting and/or disrupting individual and group knowledge in order to gain advantage" [10]. NATO's strategy is defensive, focusing on strengthening the cognitive infrastructure of its member states. The primary objective is to build societal resilience. This approach is consistent with the concept of deterrence by denial, which aims to deter an attack by making it unlikely to succeed. The creation of a dedicated cognitive warfare concept within a military command (ACT) marks a major bureaucratic and philosophical shift in NATO, recognizing that societal cohesion is now a formal military-strategic issue. Traditionally, military commands have focused on kinetic operations and physical domains, while societal issues are the responsibility of political authorities. The creation of an Applied Cognitive Effects (ACE) team within HQ SACT and the assignment of ACT to develop a military concept of cognitive warfare formalizes the idea that the cognitive space is a domain of military operations. This blurs the lines between civilian and military responsibilities. NATO's military wing is now developing doctrine to defend not only its physical domains but also the cognitive space. This suggests a future in which military planning must deeply integrate socio-political analysis and where civil-military cooperation becomes a central, rather than an ancillary, component of defense strategy.

b) The doctrine of the United States – the pursuit of information superiority.

The traditional US approach to information operations (IO) is defined by its five pillars – electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOPS), military deception (MILDEC), and operational security (OPSEC). This model is often viewed as a specialized capability. The publication in 2023 of Army Publication (ADP) 3-13, "Information" [11] and the establishment of the Joint Concept for Information Advantage (JCIA) in the same year marked a significant doctrinal shift. These documents reframe information as a combat power dynamic and emphasize a combined arms approach. The central concept in the new doctrine is that every service member has a role in the information

environment – it is no longer the exclusive domain of narrow specialists. Every action, image, and statement generates information effects [12]. While the previous JCOIE concept (2018) laid the foundations for the integration of physical and information power, the new JCIA framework (2023) completes this cycle. It harmonizes the efforts of all types of armed forces, emphasizing decision superiority and shaping the behavior of participants to achieve lasting strategic results. In this context, the United States is actively developing offensive cognitive warfare capabilities, seen as a force multiplier. The goal is to achieve cognitive dominance through narrative dominance [13]. In the defensive plan, the theory of information inoculation (“pre-bunking”) is applied. Through it, supported by artificial intelligence systems, military personnel build cognitive resilience against disinformation in real time [14].

c) Russian Doctrine – The Art of Reflective Governance.

Reflexive control is defined as a means of transmitting specially prepared information to an adversary in order to induce him to voluntarily make a predetermined decision that is advantageous to the initiator [15]. The goal is to control the adversary’s decision-making process itself. The main mechanism is the manipulation of key factors in the adversary’s perception of the world so that he logically reaches the desired conclusion. Russia implements reflexive control as a holistic, continuous strategic effort, conducted in both peacetime and wartime. It is not a separate line of action, but is integrated with kinetic, diplomatic, and economic actions. Reflexive control is not a reactive measure, but a doctrine of prevention, which is inherently a long-term shaping operation. Therefore, it is not simply a wartime tactic, but a strategic approach to international relations. This method views cognitive space as a constant battlefield, where the goal is to continuously degrade the adversary’s decision-making autonomy, thereby preventing effective resistance. The Russian model of cognitive warfare is deeply integrated with its intelligence services and state structure, giving it a unity of effort that decentralized, democratic alliances find difficult to effectively counter. Russia can execute a holistic, long-term cognitive strategy with a single goal, while Western responses are often fragmented, slower, and constrained by legal and political divisions. This is a structural advantage for Russia in the cognitive domain.

d) Chinese Doctrine – From the Three Wars to Intelligent Warfare and Cognitive Domination.

The foundation of the Chinese approach is the Three Wars doctrine, formally adopted in 2003. This doctrine integrates three interrelated strategies that are applied continuously in both peacetime and wartime – public opinion warfare, psychological warfare, and legal warfare [16]. With the development of technology, especially artificial intelligence, Chinese military thought has evolved towards the concept of intelligentized warfare [17]. In this new paradigm, the cognitive domain is seen as the decisive battlefield, even more important than the physical domains. Chinese strategists argue that whoever controls the

cognitive domain can achieve victory by directly influencing the adversary’s brain, its emotions, motives, and decisions. This approach integrates the Three Wars with the latest advances in neuroscience, artificial intelligence, big data, and social media to achieve cognitive control or mind domination. The goal is to achieve strategic advantage by shaping perceptions and destabilizing adversary societies even in peacetime. The Chinese approach is holistic and encompasses the whole of government, blurring the lines between military and civilian, peace and war [18].

The differences between the approaches of the countries examined to cognitive warfare are significant. They are rooted in different strategic cultures, political systems, and philosophies of warfare. NATO’s core strategic logic is resilience. Their concept is defensive, focused on strengthening society to resist attack. It is reactive and prioritizes preserving the integrity of the democratic system. The US approach is focused on gaining and maintaining the initiative. It is proactive and views the information environment as a domain of continuous struggle for better position and gaining advantage. The Eastern school applies a holistic approach. The Russian concept is offensive, focused on manipulating and undermining the will of the adversary. It is preventive and aims to completely dominate the adversary’s decision-making process. China applies a concept focused on achieving cognitive control and victory without fighting. It is comprehensive, long-term, and integrates all instruments of national power. The goal is to shape the strategic environment in one’s favor to achieve dominance.

C. *Integrating cognitive warfare into operational art*

The very definition of operational art as a cognitive approach means that it is inherently the framework for conducting cognitive warfare. Military planning, especially at the operational level, is a cognitive process of understanding complex, unstructured problems and designing solutions. The connection between operational art and cognitive warfare is that all military outcomes are ultimately cognitive. The moment one side accepts that it has been defeated, regardless of its remaining physical capacity, is defeat. This is a cognitive state. Even humanitarian operations depend on the perceptions and decisions of the population being assisted. Therefore, the cognitive dimension – defined as the mind of the decision maker or a specific audience – is the terrain on which information functions are conducted. Operational art must plan operations that purposefully shape this terrain.

The transition from a doctrinal concept to an operational application of cognitive warfare requires changes in the way operations are planned. Operational design is the conceptual component of planning. It helps the commander understand the environment, define the problem, and develop a broad operational approach before detailed planning begins. It is at this stage that cognitive goals must be formulated. Rather than focusing solely on physical end states, operational designers must define the desired cognitive end state. By defining the problem in

cognitive terms, operational design can guide planning toward identifying nonphysical centers of gravity. Traditionally, the center of gravity has been sought among physical objects – enemy forces, command centers, key infrastructure. In the cognitive era, the center of gravity is increasingly shifting to intangible factors – public opinion in the adversary state, the political will of its leadership, the unity of a given military alliance, or even trust in the economic system. Integrating cognitive warfare requires modifications to the operational planning process. Mission analysis must be expanded to provide a deeper understanding of cultural narratives, social norms, psychological vulnerabilities, key influencers, and information pathways of target audiences. When developing options for action (COA), headquarters should include cognitive lines of effort as core components, not add-ons. A COA can synchronize a physical maneuver, a cyberattack, and a targeted disinformation campaign to disrupt an adversary's decision-making. COA analysis is the most challenging. It is essentially an evaluation of maneuver and firepower. Influence wargaming is fundamentally different. It must simulate human factors such as attitudes, behavior, motivation, media influence, and the spread of disinformation. These games must account for uncertainty and rapidly changing attitudes, making impact assessment extremely difficult. Modeling human decision-making is a complex task for which current tools are often inadequate. The problem with war games translates directly to the assessment of cognitive influence in real-world operations, with the main difficulty being the limited tools. [8]. Bazalgette and Janin propose a measure of cognitive entropy – a measure of information chaos and the breakdown of shared narratives in a given society. This approach identifies seven cognitive domains – national belonging; moral ecology; social norms; historical memory; institutional legitimacy; strategic autonomy and interethnic cohesion. Their interaction can be mapped to identify cognitive instability. In this model, artificial intelligence can play an observational role, detecting changes in narratives and measuring cognitive transitions, supporting human analysis [19].

Multi-domain operations (MDO) is the current operational concept of the United States and NATO, which emphasizes the synchronization of military activities across all operational domains (land, air, sea, space and cyberspace). The integration of cognitive warfare raises a fundamental doctrinal question – is the cognitive dimension simply an effect that manifests itself in all domains, or is it its own, separate domain? The NATO Warfighting Capstone Concept (NWCC) introduces the imperative of Cognitive Superiority. The document explains that future conflicts will be characterized by a fusion of dimensions, and the ability to understand and influence the cognitive sphere will be crucial to victory [20]. With AJP-01 (Allied Joint Doctrine), NATO officially introduces the concept of MDO. The doctrine states that NATO forces operate in five domains – Maritime, Land, Air, Space and Cyberspace, but their goal is to generate effects in three dimensions – physical, virtual and cognitive [21]. The Allied Joint Doctrine for Information Operations (AJP-10.1) explicitly states that the information environment is a layered battlefield composed

of these three dimensions. It defines the cognitive dimension as the critical dimension because, ultimately, every physical action aims to change the behavior or decision of the adversary [22]. These NATO doctrinal documents suggest that actions in the five physical and virtual domains generate effects in the physical, virtual, and cognitive dimensions. The US military openly states its desire for cognitive dominance as a key factor in MDO. NATO's concept of cognitive warfare also treats it as a battlefield. Some analysts and military structures support the establishment of a cognitive domain. However, there is a strong counterargument that the addition of a cognitive domain unnecessarily complicates military planning. This argument argues that cognitive effects are so strongly intertwined with all other domains that they cannot be isolated. According to this perspective, cognitive aspects are better managed within the information domain or as an integral part of planning in any other domain [23].

Regardless of the doctrinal debate, the consensus is that modern operational art must be concerned with the synchronization of cognitive effects. It becomes the art of creating convergent dilemmas – using the speed and integration of combat networks to overload the adversary's decision-making cycle by attacking not only its physical infrastructure but also its cognitive integrity.

Integrating cognitive warfare into operational art is fraught with enormous challenges, both in offensive and defensive operations. The very act of planning for cognitive warfare exposes staffs to the risk of cognitive overload. Human cognition is a finite resource. Adding the extremely complex and uncertain cognitive dimension to an already busy planning process can lead to analysis paralysis, mental fatigue, and ultimately worse, less flexible plans. The more complex the problem, the more likely it is that people will resort to suboptimal strategies. The use of artificial intelligence can be a powerful weapon in conducting cognitive warfare and a key tool in dealing with it. It can take on the heavy lifting, quickly analyze and compare COAs, and present commanders with predictions of alternative future events, thereby reducing cognitive load and enabling better decision-making.

IV. CONCLUSIONS

This paper examines the transformation of operational art in the context of cognitive warfare through a systematic and comparative analysis of leading military doctrines. Internal differentiation within the Western bloc is revealed. While the NATO model is defined as reactive-defensive, focused on building shared cognitive resilience, the US model is markedly proactive and offensive-oriented, striving to achieve cognitive dominance and information superiority by actively shaping the perceptions of the enemy. The Eastern model is proactive-offensive, aimed at complete domination over the enemy's decision-making processes. It is established that cognitive warfare reformulates the concept of defeat. It is no longer defined by the physical destruction of forces, but as cognitive paralysis – a state in which the subject loses the will to resist and the ability to rationally manage. The analysis enters the role of artificial intelligence and big data as factors that industrialize cognitive influence. The

conclusion is that digital hyper-connectivity is turning the very architecture of modern society into its greatest strategic vulnerability. The integration of cognitive warfare into operational art represents its next evolutionary phase. The cognitive dimension is not simply an additional effect, but the critical space in which the outcome of modern MDOs is decided. Decisive success no longer depends solely on physical maneuvering, but on achieving cognitive superiority through the synchronization of physical, virtual, and psychological effects. A doctrinal adaptation is needed so that cognitive lines of effort are embedded as an integral part of military decision-making and operational design, rather than as isolated ancillary functions. An interdisciplinary approach is recommended in future research and command training to bring together military science, cognitive psychology, neuroscience, and data analytics to more accurately map the cognitive environment. It is critically important to create new scientific methods for measuring the effect in the cognitive domain, which will replace traditional quantitative indicators with qualitative analyses of behavioral changes. To form strategic resilience, at the national security level, it is recommended to invest in cognitive inoculation through education and civil-military cooperation, which will protect society from algorithmically automated disinformation.

REFERENCES

- [1] O. Backes and A. Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States," Belfer Center for Science and International Affairs, Nov. 2019. [Online]. Available: <https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states>. [Accessed: Feb. 9, 2026].
- [2] T.-C. Hung and T.-W. Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," *Journal of Cybersecurity*, vol. X, no. X, Jul. 2022. [Online]. Available: <https://www.researchgate.net/publication/362163528>. [Accessed: Feb. 10, 2026].
- [3] NATO ACT, "Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against 'Cognitive Warfare'," July 3, 2024. [Online]. Available: <https://www.act.nato.int/article/cogwar-concept/>. [Accessed: Feb. 10, 2026].
- [4] S. Miller, "Cognitive warfare: an ethical analysis," Sept. 2023. [Online]. Available: https://www.researchgate.net/publication/373656135_Cognitive_warfare_an_ethical_analysis. [Accessed: Feb. 10, 2026].
- [5] B. Tashev, M. Purcell, and B. McLaughlin, "Russia's Information Warfare Exploring the Cognitive Dimension," 2019. [Online]. Available: <https://apps.dtic.mil/sti/pdfs/AD1101048.pdf>. [Accessed: Feb. 10, 2025].
- [6] M. Ninov, R. Borisova, and S. Dragova, "The Art of Perception: China's Vision of Cognitive Influence and Its Implications for Global Security," 2023. [Online]. Available: <https://www.academia.edu/>. [Accessed: Feb. 5, 2026].
- [7] F. Hansen, "When Russia Wages War in the Cognitive Domain," *The Journal of Slavic Military Studies*, vol. 34, no. 4, Dec. 16, 2021. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/13518046.2021.1990562>. [Accessed: Feb. 10, 2026].
- [8] B. Clavier and F. du Cluzel, "The Cognitive Warfare Concept," Jan. 2022 (updated Dec. 2023). [Online]. Available: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Clavier-du-Cluzel-final_0.pdf. [Accessed: Feb. 10, 2026].
- [9] NATO StratCom Centre of Excellence, "About Strategic Communications," n.d. [Online]. Available: https://stratcomcoe.org/about_us/about-strategic-communications/1. [Accessed: Feb. 10, 2026].
- [10] NATO ACT, "Cognitive Warfare: Strengthening and Defending the Mind," Apr. 5, 2023. [Online]. Available: <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/>. [Accessed: Feb. 10, 2026].
- [11] Headquarters, Department of the Army, "ADP 3-13 Information," Nov. 27, 2023. [Online]. Available: https://rdl.train.army.mil/catalog-ws/view/100.ATSC/B704630A-BF73-4EA5-8994-9EE4E300269B-1701200317950/adp3_13.pdf. [Accessed: Feb. 11, 2026].
- [12] R. Creed and M. Flynn, "Information Advantage: A Combined Arms Approach," *Military Review*, May-June 2024. [Online]. Available: <https://www.armyupress.army.mil/Journals/Military-Review/>. [Accessed: Feb. 11, 2026].
- [13] E. Annett and J. Giordano, "The 'Ins' and 'Outs' of Cognitive Warfare: What's the Next Move?," June 16, 2025. [Online]. Available: <https://inss.ndu.edu/Media/News/Article/4217626/>. [Accessed: Feb. 11, 2026].
- [14] R. Bebbler, "Information Inoculation: Preparing US Warfighters for Cognitive War," Hudson Institute, Sept. 29, 2025. [Online]. Available: <https://www.hudson.org/national-security-defense/information-inoculation>. [Accessed: Feb. 11, 2026].
- [15] D. Nord and A. Rinaldi, "What Is Cognitive Warfare and Why Does It Matter for You?," *Greater Good Magazine*, Aug. 8, 2025. [Online]. Available: <https://greatergood.berkeley.edu/>. [Accessed: Feb. 10, 2026].
- [16] M. Martin, "China's Three Information Warfares," *Proceedings*, vol. 147/3/1,417, Mar. 2021. [Online]. Available: <https://www.usni.org/magazines/proceedings/2021/march/chinas-three-information-warfares>. [Accessed: Feb. 12, 2025].
- [17] K. Takagi, "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine," Hudson Institute, June 22, 2022. [Online]. Available: <https://www.hudson.org/national-security-defense/the-future-of-china-s-cognitive-warfare>. [Accessed: Feb. 12, 2026].
- [18] J. Baughman, "How China Wins the Cognitive Domain," China Aerospace Studies Institute, Jan. 2023. [Online]. Available: <https://www.airuniversity.af.edu/CASI/>. [Accessed: Feb. 12, 2026].
- [19] D. Bazalgette and P. Janin, "Cognitive warfare: what seven years of military-civilian research reveals," *Polytechnique Insights*, Nov. 5, 2025. [Online]. Available: <https://www.polytechnique-insights.com/en/columns/society/cognitive-warfare-what-seven-years-of-military-civilian-research-reveals/>. [Accessed: Feb. 13, 2026].
- [20] NATO ACT, "NATO Warfighting Capstone Concept (NWCC)," 2021. [Online]. Available: <https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/>. [Accessed: Feb. 13, 2026].
- [21] NATO Standardization Office, "Allied Joint Doctrine (AJP-01)," Ed. F, Ver. 1, Dec. 2022. [Online]. Available: [https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_\(1\)_2437.pdf](https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf). [Accessed: Feb. 13, 2026].
- [22] NATO Standardization Office, "Allied Joint Doctrine for Information Operations (AJP-10.1)," Ed. A, Ver. 1, Jan. 2023. [Online]. Available: <https://assets.publishing.service.gov.uk/>. [Accessed: Feb. 13, 2026].
- [23] P. Hofstetter and F. Jossen, "There Is No Need For A Cognitive Domain," *The Defense Horizon Journal*, Nov. 2, 2023. [Online]. Available: <https://tdhj.org/blog/post/no-need-cognitive-domain/>. [Accessed: Feb. 13, 2026].

A Conceptual Model for Risk Management in Hybrid Threats and Cognitive Attacks

Milko Stefanov

Rakovski National Defense College
Sofia, Bulgaria
m.j.stefanov@rndc.bg

Abstract— This report presents an integrated conceptual model for risk management, adapted to the specifics of hybrid threats and cognitive warfare. In the conditions of a changed strategic environment, where the objects of attack are not only physical assets, but also human consciousness and social cohesion, traditional risk assessment models prove to be insufficient. The report analyzes the essence of cognitive attack at the biological, psychological and social levels, considering the influence of technologies such as artificial intelligence and algorithmic sabotage. Qualitative risk indicators are presented through the OODA (Observe, Orient, Decide, Act) loop and NATO's "The House" model. The central place is occupied by the proposed conceptual model for quantitative transformation of cognitive risk, based on institutional vulnerability, media amplification and cognitive resilience of society.

Keywords— *hybrid threats, cognitive warfare, risk management, cognitive resilience.*

I. INTRODUCTION

The modern strategic environment marks a transition from conventional conflicts to multidimensional hybrid strategies operating below the threshold of armed conflict. At the center of this paradigm is cognitive warfare, aimed at paralyzing the will to resist and destroying public consensus by manipulating perceptions. For countries like Bulgaria, located in a geopolitically sensitive region, it is critically important to have an adequate framework for analyzing these asymmetric impacts. The purpose of the development is to define and substantiate an integrated conceptual model for risk management, which allows the transformation of qualitative indicators of cognitive attacks into quantitative values for the needs of strategic planning of national security. The working hypothesis is that the construction of effective national resilience against hybrid threats is possible only by moving from traditional physical metrics to a complex assessment of cognitive risk, uniting institutional readiness, the technological influence of the

information environment and the psychological immunity of society.

II. MATERIALS AND METHODS

To achieve the objectives of the report, a multidisciplinary approach was used, including:

Theoretical analysis and synthesis - study of NATO doctrinal documents and concepts of strategic competitors.

Comparative analysis - comparison between traditional information operations and the essence of cognitive warfare.

Modeling - use of the OODA (Observe, Orient, Decide, Act) cycle to identify qualitative risk indicators and application of the DISARM framework for threat taxonomy.

Assessment methodology - combining the expert assessment method (using a 5-point scale) with statistical processing of sociological data to calculate cognitive resilience.

Systemic approach - analysis of the national security architecture of Bulgaria through the prism of the "three lines of defense" model.

III. RESULTS AND DISCUSSION

A. Cognitive warfare – essence and forms of manifestation

Unlike traditional information operations (InfoOps) or psychological operations (PsyOps), which are usually limited in time and aim for short-term penetration of specific messages, cognitive warfare seeks deep, lasting, and often irreversible changes in the cognitive patterns, behavioral dispositions, risk perception, and civic cohesion of the adversary.

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.46>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

The NATO Chief Scientist's report on cognitive warfare [1] distinguishes three main levels of influence that hybrid state and non-state actors systematically exploit. The biological level targets the nervous system as the physical and focal basis of thought, emotion and behaviour. Offensive actions here include the induction of physiological stress, sensory overload and the potential use of neurotechnologies to disrupt sleep, concentration and the basic combat capability of personnel. At the psychological level, the focus is on influencing cognitive appraisal, emotional framing and the exploitation of existing human vulnerabilities and cognitive biases. Here, attackers exploit phenomena such as in-group/out-group polarization, confirmation bias and emotional priming to shape individual and collective attitudes, beliefs and judgements in their favour. The social level is the macro level of cognitive warfare, where the goal is to destroy social cohesion. Attacks are aimed at undermining trust in democratic authorities, delegitimizing institutions, eroding alliance commitments, and dividing society by instilling chronic doubt and cynicism.

The forms of manifestation of cognitive attacks are extremely diverse, adaptive and strongly determined by the speed of technological development. Artificial intelligence (AI) acts as an accelerator and multiplier of the power of cognitive attack. It allows the creation of the so-called synthetic credibility on an industrial scale. This is achieved by generating deep fakes, creating synthetic experts with fake academic profiles and distributing forged evidence that is visually and logically indistinguishable from reality for the average user. Algorithmic sabotage is another advanced form of manifestation. In it, the hybrid adversary does not limit itself to creating disinformation, but actively interferes with information architectures and flows. This includes "poisoning" machine learning databases (data poisoning / LLM poisoning), which introduces adversarial noise into the algorithms that societies, intelligence and military structures rely on for situational awareness [2]. The goal is to compromise the integrity of command and control systems by generating false recommendations or distorting the decision-making process.

The experience and doctrinal documents of NATO's strategic competitors demonstrate the systematic and resource-rich integration of these methods. The Russian Federation uses a complex combination of communication technologies, cyberattacks and perception manipulation operations to build cognitive traps. They aim to provoke either strategic overreaction or complete paralysis and indecision among decision-makers in the Alliance [3]. The Russian approach to hybrid warfare actively exploits the discrepancy in reaction thresholds of democratic societies. The People's Republic of China conceptualizes cognitive warfare through its Three Warfares strategy, which involves the use of public opinion, psychological operations and lawfare to achieve political and military victories without the need for open kinetic confrontation [4]. As technology advances, this strategy has evolved into the concept of intelligent warfare [5].

The European Centre for Countering Hybrid Threats (EU Hybrid CoE) conceptualizes these processes in the civilian sector as cognitive intrusion. It is defined as the

deliberate manipulation of collective mental processes that relies on nurturing a culture of disinformation and inflaming negative emotions of anger to circumvent normal channels of democratic political expression and provoke political violence [6].

B. Qualitative indicators in assessing the risk of cognitive attacks

Assessing risk in the cognitive domain requires moving away from traditional metrics, such as media coverage, impressions, or share volume, to more in-depth metrics that focus on the quality, speed, and integrity of decision-making. To identify which quality metrics actually impact risk, the academic and military communities, and NATO research teams in particular, have developed several specialized theoretical frameworks [7].

One of the most applicable and comprehensive theoretical models for analyzing cognitive vulnerabilities is the interactive framework based on the OODA loop. This framework views cognitive warfare not as a one-way media campaign, but as an adaptive, continuous race between attacker and defender to gain advantage in the decision-making cycle. The model identifies qualitative indicators over time horizons – acute effects that lead to immediate degradation within minutes or days, and chronic effects that accumulate over months and years [8].

Risk assessment through the OODA loop allows the identification of specific offensive effects and corresponding countermeasure indicators at each decision-making phase:

Observe – In this initial phase, the attacker seeks information saturation, noise generation, and selective deception to disrupt shared situational awareness. Key risk indicators here include the ability of institutions to correctly assess the credibility of information, the degree to which accurate observation is maintained, and susceptibility to information overload.

Orient – Here, efforts are directed toward emotional framing, exploitation of prejudice, and erosion of institutional trust through the creation of ambiguity. Resilience is measured by the capacity for collective meaning-making of events and the effectiveness of calibrating trust between official channels and unauthorized sources.

Decide – The attack aims to induce strategic hesitation, confusion, undue overconfidence, or complete paralysis of will. Risk indicators include decision latency (delay compared to the norm), frequency of canceled orders, and inadequate changes in confidence thresholds when making choices.

Act – In the final phase, the adversary provokes premature, inappropriate, or intentionally passive actions that serve its interests. Indicators of breakthrough are the degree of deviation from the initial operational concept and the missed time windows for tactical or political execution. This transition from qualitative to quantitative dimensions is essential for transforming the model into a working tool for national security.

In parallel to the OODA model, NATO's Science and Technology Organisation (STO) developed "The House Model" for mitigating and responding to cognitive warfare. This model maps human cognition through seven key domains that function as metrics for vulnerability and resilience. The model consists of three vertical Pillars and four horizontal intersecting Bars:

- Pillars of vulnerability – cognitive neuroscience, cognitive and behavioural science, social and cultural science. The risk increases proportionally to the extent to which an adversary can penetrate these scientific domains and turn them against the defender.

- Horizontal multipliers – situational awareness and sensemaking, cognitive effects, *modus operandi*, and technological force multipliers [9].

Any registered weakness or breach in these pillars represents a primary qualitative indicator that the relevant organization or society is at high risk of a successful cognitive hack.

For operational intelligence purposes, a NATO research team integrated the General Morphological Analysis (GMA) and the Disinformation Risk Analysis and Management Framework (DISARM) to create a structure of Indicators and Warnings (I&W). The DISARM framework, based on the logic of the MITRE ATT&CK cyber model, catalogs specific tactics and techniques that serve as qualitative diagnostic indicators. The DISARM Red Framework identifies indicators in the planning, execution, and evaluation stages of a campaign. The main qualitative indicators here are the creation of clusters of inauthentic social media profiles, the generation of micro-targeted clickbait, the systematic exploitation of historical or local traumatic narratives, and temporal anomalies in cyberspace [7]. The main challenge facing classical risk management, however, lies in the fact that these listed indicators – decision latency, institutional trust, emotional reactivity, social cohesion – are extremely qualitative, fuzzy, subjective and difficult to measure with conventional methods. To be useful in the defense planning process, they must undergo a precise quantitative transformation.

C. A conceptual model for risk management in hybrid threats and cognitive attacks

The national security architecture of the Republic of Bulgaria is a complex system of institutions, regulations, strategic documents and operational procedures, the purpose of which is to protect national interests. It is built on the principles of democratic control, the rule of law and the separation of powers, but at the same time it is faced with the imperative need to increase its flexibility and speed of response. A fundamental element in the management of national security in the Republic of Bulgaria is the cycle of strategic planning, monitoring and accountability. This cycle is most clearly implemented through the annual report on the state of national security, which is prepared by the executive branch and submitted for consideration and approval by the legislative body. This document performs several critical functions

simultaneously – it serves as a diagnostic tool for identifying existing vulnerabilities, functions as a platform for accountability for actions taken to date and represents a roadmap for future initiatives. The report aims to present a detailed description of the measures that state-level institutions plan to take in the coming period in order to proactively counter the diagnosed challenges and exploit emerging opportunities [10]. This planning requires an extremely high level of coordination between the different ministries and agencies. The executive branch in Bulgaria is responsible for the operational counteraction to malicious influence, which requires a continuous analysis of the effectiveness of national security policy. Despite the existence of this structured planning cycle, a practical analysis of institutional interaction reveals certain structural deficiencies. Fragmentation of efforts is often observed, in which different departments approach hybrid threats through the prism of their narrow specialization, without taking into account the full scale of the cognitive impact. For example, technical agencies focus exclusively on the integrity of networks, while information directorates analyze the media environment, but the synthesis between these two data streams is often not fast enough to prevent the deployment of a complex cognitive attack. In the context of risk management and ensuring resilience against hybrid attacks, Bulgarian state institutions adapt and apply the conceptual framework of the three lines of defense [11]. This framework is designed to provide a structured approach to risk management through a clear allocation of responsibilities:

- First line – operational managers, who own the processes and are directly responsible for managing risks in their daily activities.

- Second line – oversight and risk management functions, which set policies, standards and carry out monitoring.

- Third line – independent internal and external audit, which provides an objective assessment of the effectiveness of the first two lines.

Despite its theoretical robustness, the implementation of this framework in the Bulgarian state administration often encounters three common problems identified in contemporary security architecture research. These problems include the lack of clear communication between lines, the blurring of responsibilities in the event of complex, multi-domain incidents, and the insufficient expertise of the first line to recognize subtle cognitive or social engineering attacks. These structural weaknesses create blind spots in the security architecture through which foreign malicious influence can penetrate and spread before being detected by monitoring systems. In order for the Bulgarian security architecture to be effective in the context of cognitive impacts, it is necessary to analyze its current critical vulnerabilities. Despite the declared intentions in the annual reports on the state of national security, the system continues to demonstrate weaknesses that make it susceptible to hybrid impacts. These vulnerabilities can be conceptualized through the academic formula of cognitive risk

$$R_c = \frac{V_i \cdot A_m}{C_r} \quad (1)$$

where:

R_c – cognitive risk;

V_i – institutional vulnerability;

A_m – algorithmic and media amplification of the attack;

C_r – cognitive resilience of society.

The cognitive risk formula is a conceptual model. It does not use a specific mathematical law with precise numerical dimensions, but is an adaptation of the classical academic equation for assessing risk in security and management, applied specifically to the mechanisms of cognitive warfare. In Bulgarian practice, in internal audit and risk management methodologies in state administration, the basic formula for quantitative assessment is most often used:

$$Risk = Probability \times Impact \quad (2)$$

In more detailed national security models, this concept is often expanded to the logic:

$$Risk = \frac{Vulnerability \times Threat}{Threat mitigation capacity} \quad (3)$$

Thus, the formula serves as a theoretical model that translates standard risk management principles into the language of modern information and psychological threats. Since this is a qualitative model, the values for individual variables are not calculated mathematically, but are obtained through a qualitative strategic analysis of processes in the state and society.

Institutional vulnerability (V_i) is assessed based on the existing structural deficiencies in the state architecture. It is high when problems such as poor implementation of the three lines of defense framework in the administration and lack of capacity for preventive identification and neutralization of latent vulnerabilities in digital systems are observed.

Algorithmic and media amplification of the attack (A_m) reflects the role of the information environment as a catalyst for the threat. Its value increases when the media ecosystem uncritically reproduces the narratives of the attacking actors, leading to distorted perceptions of systemic vulnerabilities, increased public anxiety, and erosion of institutional trust.

Cognitive resilience of society (C_r) is measured by the ability of society to resist psychological operations. Resilience is low when certain groups are highly susceptible to manipulations such as linguistic hacking, in which emotionally charged keywords are injected to activate historical traumas and incite civil disobedience.

This model illustrates the strategic logic that in order to reduce the overall cognitive risk to national security, Bulgarian institutions must simultaneously minimize their own structural weaknesses and the influence of the disinformation environment, while simultaneously building high psychological immunity in society.

To transform qualitative assessment into quantitative, the most adequate results would be obtained by a combined approach that integrates the method of expert assessments and sociological surveys. The method of expert assessments is considered one of the most up-to-date and reliable methods for deriving quantitative values based on primary qualitative information. In the practice of Bulgarian institutions, this method is often applied through the use of a 5-point rating scale (from 1 - “very low”, to 5 - “very high”), through which specialists assess the effectiveness and interaction in a given system. Institutional vulnerability (V_i) can be assessed by independent auditors and security experts, who can give a numerical assessment of structural deficiencies. Media amplification (A_m) can be assessed by open source analysts (OSINT) and communication experts, who can score the scale of dissemination of a given disinformation. To increase accuracy, the expert assessment method can be successfully combined with the conduct of simulation models and exercises that test how employees respond to crises, allowing for a more objective assessment of their actions. Surveys and statistical processing are applicable to the calculation of the denominator – the cognitive resilience of society (C_r), where expert assessments are not sufficient. Here, the application of nationally representative surveys is absolutely necessary. Through statistical processing of citizens’ responses, accurate numerical coefficients can be derived, reflecting the levels of public trust in institutions, susceptibility to fake news and emotional reactivity to hybrid narratives. A similar approach to converting qualitative indicators into numerical values has already been established in the Bulgarian administration in the management of other types of risk, in which the level is calculated by multiplying the numerical assessment of the severity of the impact by the probability of occurrence. The resulting result falls within predefined numerical limits for low, medium or high risk levels. Similarly, by creating a standardized matrix based on expert assessments (scale from 1 to 5) and sociological data, the cognitive risk formula can be transformed from a conceptual model into a fully functional mathematical tool for the executive branch.

For the purpose of practical testing and to ensure the compatibility of the model with established practices in internal audit, the variables are assessed using the expert assessment method, combined with open source intelligence (OSINT) and representative sociological surveys. Table I shows how a standardized 5-point scale (from 1 to 5) is used. For the variables V_i and A_m , a score of 1 means the least pronounced factor (best case scenario) and 5 means the most pronounced factor (worst case scenario). Conversely, for the variable C_r (resilience), a score of 1 means the least pronounced factor (worst case scenario) and a score of 5 means the most pronounced factor (best case scenario).

TABLE I: FIVE-POINT SCALE FOR DETERMINING VARIABLE VALUES IN RISK ASSESSMENT

Rating	V_i	A_m	C_r
1	Optimal interdepartmental coordination,	Isolated and fragmented cases of	A total collapse of the social contract,

Rating	Vi	Am	Cr
	available AI tools for real-time detection, an effective strategy.	disinformation, relying only on organic reach, complete lack of AI.	organized mass protests generated entirely on the basis of disinformation.
2	Availability of basic procedures and action plans, but with a recorded slow response; partial coordination.	Localized campaigns, using traditional troll farms with easily recognizable handwriting.	Systemic distrust of authority, extremely high political polarization, dominant public apathy
3	Presence of serious institutional blind spots, fragmented implementation of controls.	Synchronized campaigns operating across multiple platforms simultaneously, successful micro-targeting.	A divided society, tangible presence of historical traumas, susceptibility to conspiracy theories.
4	Deep structural fragmentation, lack of an up-to-date national strategy, dysfunctional regulators.	Large-scale and resource-secured use of GenAI (deepfakes), automated saturation of the info-space.	Stable trust in key government bodies, moderate public reaction to emotional manipulation.
5	Complete institutional paralysis, inability to make decisions, penetration of foreign influence.	AI-Enhanced Reflexive Control (AIRC), complete takeover of the national information flow.	Extremely high public trust in institutions and the media, strong social consensus on strategic topics.

The calculation of the ultimate risk (Rc) generates a numerical value ranging from 0.2 to 25, as shown in Table II. This scale allows the categorisation of risk into four strategic quadrants that dictate the required response.

TABLE II: RISK LEVEL AND RESPONSE

Scope (Rc)	Risk level	Strategic response	Main subjects
0,2-0,4	Low	Standard monitoring and data collection.	First line of defense.
4,1-10	Moderate	Preventive communication campaigns and enhanced surveillance.	Compliance functions.
10,1-18	High	Interdepartmental coordination and active countermeasures.	Independent audit and specialized units.
18,1-25	Critical	Emergency restructuring and protection of national security.	State leadership and Security Council.

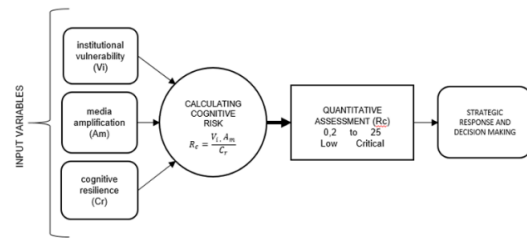


Fig. 1. Schematic representation of the cognitive risk (Rc) assessment model.

Fig. 1 presents the logical and mathematical relationship between the input data, the calculation process and the strategic result. The main interrelationships it highlights are the directly proportional dependence of cognitive risk (Rc) on institutional vulnerability (Vi) and media amplification (Am), which work in synchrony. If institutions are weak and the media campaign is large-scale, the risk increases exponentially. An inversely proportional dependence on cognitive resilience (Cr) is presented as a regulator. Even with high vulnerability and a strong attack, a high level of resilience of society can drastically reduce the final risk. Subjective categories, such as media influence or public fear, are transformed into a specific numerical value, which is not an end in itself, but a basis for decision-making.

In the proposed conceptual model, the values of the variables are not summed, but interact multiplicatively, which reflects the asymmetric nature of cognitive warfare. When we define a value of 4 (high) for Am, this means that the information ecosystem uncritically reproduces foreign narratives that distort perceptions of systemic vulnerabilities. Advanced technologies such as AI are used to generate synthetic credibility and deep fakes on an industrial scale. Algorithmic selection of social networks creates “echo chambers” that accelerate the spread of disinformation. When this amplification is combined with 2 (low) for Cr, a defense collapse effect is observed. Since Cr is in the denominator of formula (1), low resilience sharply increases the ultimate risk. At a value of 2, society is highly susceptible to linguistic hacking, in which emotionally charged keywords activate historical traumas and incite civil disobedience. The combination of massive pressure (value 4) and weak immunity (value 2) leads to cognitive intrusion, which bypasses normal channels of democratic expression and provokes political violence.

In order to convert qualitative responses from sociological surveys into quantitative coefficients for formula (1), it is necessary to apply a statistical normalization process. This ensures that the data from citizens are compatible with the expert assessment (scale 1–5) for Vi and Am. Questions from nationally representative surveys measuring trust in institutions, the ability to recognize fake news, and levels of social polarization are used. Each response is assigned a weight. For example, in a question about trust in the media, the response “I completely trust” receives the highest sustainability weight, and “I do not trust at all” the lowest.

The percentage values (P) are transformed into an index on a scale of 1–5 by linear interpolation:

$$Index = 1 + \left(\frac{P - P_{min}}{P_{max} - P_{min}} \right) * 4 \quad (4)$$

where:

Index – normalized value;

P – current value of the indicator;

P_{min} – minimum value of the indicator;

P_{max} – maximum value of the indicator.

The results are distributed in a matrix where:

1.00 – 1.80: Very low resilience.

1.81 – 2.60: Low resilience.

2.61 – 3.40: Moderate resilience.

3.41 – 4.20: High resilience.

4.21 – 5.00: Very high resilience.

In order to test the functionality of the conceptual model in operational conditions, the campaign against the adoption of the euro and the full economic integration of the Republic of Bulgaria into the eurozone during the period 2024–2025 was chosen as the object of the approbation [12]. This example is relevant for the purposes of the study, as it provides an illustration of the convergence between the three levels of cognitive warfare – biological, psychological and social. It also demonstrates the use of technological force multipliers, such as generative artificial intelligence and deep fakes, to manipulate mass consciousness in a member state of the European Union. Bulgaria's accession to the eurozone, initially planned for the beginning of 2024 and subsequently postponed to a later stage, has been defined as the top strategic priority of the state. During the observed period, Bulgaria is in a state of permanent political turbulence and institutional instability. Holding seven parliamentary elections in just four years has generated mass electoral apathy, deep disillusionment with the political elite, and chronic fatigue in society [13]. Disinformation researchers and analysts categorically warn that because of these factors, Bulgaria has one of the most permissive and susceptible information environments for undemocratic malicious manipulation in all of Europe [14].

The approbation process requires a quantitative assessment of the three independent variables based on the collected empirical data, expert analyses and sociological surveys, using the defined 5-point scale.

Institutional Vulnerability Score (Vi) = 4 (high). Despite the repeatedly declared intentions in the annual national security reports and the existence of an official communication strategy of the Ministry of Finance and the Bulgarian National Bank on the euro, institutional vulnerability remains extremely high. The score of 4 is justified by the following systemic deficits. The Bulgarian state has not yet adopted a comprehensive national strategy to counter disinformation. This indicates a lack of strategic leadership at the highest level. There has been

administrative and political delay in the appointment and empowerment of a national Digital Services Coordinator (DSC). This institution is the critical element for imposing regulations and sanctions on large technology platforms under the EU Digital Services Act (DSA). Without it, the state is powerless to demand the removal of coordinated hybrid networks [15]. Although the Coordination Council plans a large-scale information campaign in three phases (preparatory, substantive and de facto), its approach remains largely traditional and reactive. It is focused on conventionally informing about the benefits and refuting speculation, but institutions categorically lack the technological capacity and procedures to detect and neutralize AI-Enhanced Reflexive Control (AIRC) in real time.

Algorithmic and Media Amplification (Am) Score = 5 (critical). The distribution environment in Bulgaria has evolved from a simple communication space into a perfect catalyst for the hybrid threat. The score of 5 reflects the maximum degree of technological exploitation, justified by the proven implementation of artificial intelligence for industrial generation of micro-targeted content and textual deepfakes in Bulgarian, which successfully bypass international platform detectors [16]. The specificity of social media algorithms, which systematically prioritize content that evokes strong negative emotions, leads to immediate and viral sharing of disinformation long before any official fact-checking is possible. There is the adaptive tactic of using influencers and proxies, who do not directly create fake news, but repackage disinformation narratives in accessible formats and legitimize them to their followers [17].

Cognitive Resilience (Cr) score = 1 (very low). Cognitive resilience is assessed as extremely weak and deficient. Sociological research by the Ministry of Finance itself reveals a society that is deeply polarized and uncertain on the most important strategic issue. Despite extensive communication, while 51% of citizens support the adoption of the euro, as many as 45% are categorically against it [12]. This fragile balance provides ideal ground for hybrid exploitation. There is a systematic, deep-rooted distrust not only of the political class, but also of traditional public media. Bulgarian National Television and Bulgarian National Radio have registered a decline in trust levels in recent years, accompanied by accusations of politicization and deliberate concealment of documentaries about Russian disinformation [15]. Emotional reactivity is extremely high. Justified fear of impoverishment is combined with irrational fears of loss of identity, making the population susceptible to organized provocations. These fears materialize into real physical actions, including radical protests and attacks on diplomatic missions [18].

Applying the values of the scores for Vi, Am and Cr in formula (1), we obtain a score of 20 out of a maximum possible 25. This positions the risk categorically in the upper echelon of the “Critical Risk” quadrant. This far exceeds the tolerance threshold of conventional internal control and national security systems. The result proves that the current approach of institutions, based solely on the distribution of press releases, information brochures and traditional PR, is doomed to failure when faced with AI-

driven hybrid attacks. In order to reduce the overall risk below the critical threshold, the state faces insurmountable barriers in two of the three directions. It cannot rely on a quick and magical change in the mentality and historical burden of society, nor does it have the geopolitical power to completely turn off the algorithms of global technology platforms. Therefore, the only mathematically possible and operationally feasible way out is to focus the main effort on a drastic, uncompromising reduction of institutional vulnerability. This imperative requires a radical change in the actions of institutions, which can only be realized through a complete revision of the “three lines of defense” model.

IV. CONCLUSIONS

The proposed conceptual model for cognitive risk management allows for the transition from a purely descriptive to a predictive approach in countering hybrid threats. The integration of quantitative indicators (Vi, Am, Cy) transforms subjective perceptions of security into measurable quantities, which is critical for making timely strategic decisions. The analysis of the case study with the campaign against the euro confirms that the main weakness is not only in the intensity of the attack, but in the low cognitive resilience and institutional vulnerability. Future development of the model should focus on automating monitoring through artificial intelligence, which will allow for real-time cognitive risk assessment and more effective calibration of strategic communications.

REFERENCES

- [1] J. Giordano, "Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness," Jan. 6, 2026. [Online]. Available: <https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/>. [Accessed: Mar. 19, 2026].
- [2] R. D. Whiteside, "Narrative Manipulation, Malinfluence Operations, and Cognitive Warfare Through Large Language Model Poisoning with Adversarial Noise," Oct. 1, 2025. [Online]. Available: <https://mipb.ikn.army.mil/issues/jul-dec-2025/narrative-manipulation-malinfluence-operations-and-cognitive-warfare-through-large-language-model-poisoning-with-adversarial-noise/>. [Accessed: Mar. 19, 2026].
- [3] B. Catena, O. Ditrych, and N. Kovalčíková, "Smoke and mirrors: Building EU resilience against manipulation through cognitive security," Oct. 7, 2025. [Online]. Available: <https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive>. [Accessed: Mar. 19, 2026].
- [4] J. Baughman, "How China Wins the Cognitive Domain," Jan. 2023. [Online]. Available: <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2023-01-23%20How%20China%20Wins%20the%20Cognitive%20Domain.pdf>. [Accessed: Feb. 12, 2026].
- [5] K. Takagi, "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine," *Hudson Institute*, Jun. 22, 2022. [Online]. Available: <https://www.hudson.org/national-security-defense/the-future-of-china-s-cognitive-warfare-lessons-from-the-war-in-ukraine>. [Accessed: Feb. 12, 2026].
- [6] M. Lebrun, "Hybrid CoE Strategic Analysis 33: Anticipating cognitive intrusions: Framing the phenomenon," *European Centre of Excellence for Countering Hybrid Threats*, Jul. 2023. [Online]. Available: <https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-33-anticipating-cognitive-intrusions-framing-the-phenomenon/>. [Accessed: Mar. 19, 2026].
- [7] R. Burda, P. Buvarp, D. Brown, and M. Fitzpatrick, "Cognitive Warfare Indicators and Warnings Identification Framework," *NATO STO Meeting Proceedings*, Apr. 15, 2025. [Online]. Available: <https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-377/MP-HFM-377-09.pdf>. [Accessed: Mar. 19, 2026].
- [8] B. Rushing, W. Hersch, and S. Xu, "Cognitive Warfare: Definition, Framework, and Case Study," Mar. 6, 2026. [Online]. Available: <https://arxiv.org/pdf/2603.05222>. [Accessed: Mar. 19, 2026].
- [9] J. M. Blatny and Y. R. Masakowski, "Mitigating and responding to Cognitive Warfare," Jul. 4, 2023. [Online]. Available: [https://www.google.com/search?q=https://publications.sto.nato.int/publications/STO%2520Technical%2520Reports/STO-TR-HFM-ET-356/\\$\\$STR-HFM-ET-356-ALL.pdf&https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/\\$\\$TR-HFM-ET-356-ALL.pdf](https://www.google.com/search?q=https://publications.sto.nato.int/publications/STO%2520Technical%2520Reports/STO-TR-HFM-ET-356/$$STR-HFM-ET-356-ALL.pdf&https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/$$TR-HFM-ET-356-ALL.pdf). [Accessed: Mar. 19, 2026].
- [10] Council of Ministers of the Republic of Bulgaria, "Report on the State of National Security of the Republic of Bulgaria in 2024," 2024. [Online]. Available: <https://www.parliament.bg/bills/51/51-602-00-7.pdf>. [Accessed: Mar. 9, 2026].
- [11] The Institute of Internal Auditors, "The IIA's Three Lines Model," Jul. 2020. [Online]. Available: <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf>. [Accessed: Mar. 19, 2026].
- [12] E. MacLachlan, "Bulgaria prepares to join eurozone amid fears of Russian-backed disinformation," *The Guardian*, Oct. 28, 2025. [Online]. Available: <https://www.theguardian.com/world/2025/dec/28/bulgaria-eurozone-russia-disinformation-economy>. [Accessed: May 8, 2026].
- [13] R. Margova, "The disinformation landscape in Bulgaria," *EU DisinfoLab*, Nov. 17, 2025. [Online]. Available: <https://www.disinfo.eu/publications/disinformation-landscape-in-bulgaria/>. [Accessed: May 8, 2026].
- [14] E. Nilsson-Julien, "Bulgaria prepares for disinformation ahead of snap elections," *Euronews*, Apr. 16, 2026. [Online]. Available: <https://www.euronews.com/my-europe/2026/04/16/bulgaria-prepares-for-disinformation-ahead-of-snap-elections>. [Accessed: May 8, 2026].
- [15] V. Petrova, "BULGARIA: FRAGILE MEDIA FREEDOM PROGRESS AT RISK OF BACKSLIDING WITHOUT URGENT REFORM," *International Press Institute (IPI)*, Oct. 2025. [Online]. Available: <https://ipi.media/wp-content/uploads/2025/10/Bulgaria-Report-2025.pdf>. [Accessed: May 8, 2026].
- [16] J. Udo-Udo Jacob, "Manufacturing Dissent: The Kremlin's Digital Playbook for Destabilizing Bulgaria," *AUBG Today*, Jun. 19, 2025. [Online]. Available: <https://www.aubg.edu/aubg-today/manufacturing-dissent-the-kremlins-digital-playbook-for-destabilizing-bulgaria/>. [Accessed: May 8, 2026].
- [17] S. Nikolaeva, "Mapping Disinformation Narratives in Bulgaria: Second Working Group Report," *American University in Bulgaria (AUBG)*, May 2025. [Online]. Available: https://www.aubg.edu/wp-content/uploads/2025/07/Bulgaria-Working-Group-Report_May-2025_Mapping-Disinformation-Narratives-in-Bulgaria.pdf. [Accessed: May 8, 2026].
- [18] T. Benakis, "Parliament endorses Bulgaria's adoption of the Euro amid a harsh disinformation campaign," *European Interest*, Jun. 9, 2025. [Online]. Available: <https://www.europeaninterest.eu/parliament-endorses-bulgarias-adoption-of-the-euro-amid-a-harsh-disinformation-campaign/>. [Accessed: May 8, 2026].

Approaches for Modeling of Shopping Mall Evacuation

Svilen Stefanov

Logistics and Management Faculty
National Military University
Veliko Tarnovo, Bulgaria
sestefanov@abv.bg

Tihomir Yotkov

Logistics and Management Faculty
National Military University
Veliko Tarnovo, Bulgaria
tyotkov@gmail.com

Iliyan Lilov

Logistics and Management Faculty
National Military University
Veliko Tarnovo, Bulgaria
inl@abv.bg

Vanya Dimitrova

Research and Innovation Institute
National Military University
Veliko Tarnovo, Bulgaria
dimitrova_van@abv.bg

Abstract— This paper discusses mathematical and simulation models that could be applied to shopping mall evacuation problems. The so-called macroscopic approaches are based on dynamic network flow models. The maximum dynamic flow problem and the quickest flow problem are formulated. The so-called microscopic approaches are based on multi-agent systems. The possibilities for realistic reproduction of the processes are considered. On this basis, simple building layout is analyzed.

Keywords—quickest flow problem, maximum dynamic flow problem, multi-agent systems, shopping mall evacuation.

INTRODUCTION

Building evacuation is the process of leading people out of a building to a safe place in the shortest possible time and the safest possible manner due to the occurrence of a hazardous event. Certain crisis situations allow for a priori estimation of evacuation time, comparing it with the threat propagation time and conducting a risk analysis. In such cases, time and potential risk are key indicators.

The evacuation time consists of three components:

- Perception and awareness time: The time required for people to recognize a dangerous situation. This time depends on the reliability of the alarm system and familiarity of evacuees with emergency signals.
- Decision-making time: The time to decide on an action. It depends on the level of evacuees training.
- Movement time to the safe zone (egress time): Depends on planned evacuation procedures, architecture, physical characteristics, and human behavior under stress.

The first two components primarily depend on organizational measures and behavioral patterns, making

them difficult to reproduce analytically. Therefore, most evacuation models aim to determine the movement time to the safe zone. Factors such as the number and distribution of visitors and the throughput capacity of various sections during the process are also investigated.

Mathematical or simulation models are used for evacuation modeling; the former are typically called macromodels, while the latter are micromodels [1]. Macromodels are designed to estimate the lower bound of evacuation time. They do not account for individual differences in behavior, treating people as a homogeneous group with averaged characteristics. Modeling is reduced to formulating and solving network problems with dynamic flows. Micromodels, on the other hand, account for individual characteristics and the impact of interactions between evacuees on their movement.

The mathematical models were applied to a simplified layout of a shopping mall. The simulation model was developed within the NetLogo multi-agent systems environment. The model's capability to investigate the evacuation processes and the performance of its individual components has been verified.

DISCRETE MATHEMATICAL MODELS OF EVACUATION

To formulate optimization problems related to shopping mall evacuation, the building is represented as a directed static network. Evacuation over time is modeled using a dynamic network derived from this static one. Areas within the building with a significant occupancy are treated as source nodes in the static network. The safe zone outside the building is represented as a single sink node connected to the exits. In this sense, evacuation problems are modeled as network flow problems with multiple

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.72>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

sources and a single sink. Each node has a capacity, which is the upper bound of people it can accommodate simultaneously. Each arc is characterized by two parameters: travel time and flow capacity. The former indicates the transition time between nodes, while the latter represents the maximum number of people per unit of time through a cross-section of the arc. These two parameters can be assumed constant or treated as time-variant throughout the evacuation process. If, for instance, the passage between two zones is obstructed at a certain moment, the capacity of the corresponding arc in the dynamic network should be set to zero.

Let $G = (N, A)$ be a static network with N the set of nodes and A the set of arcs. The travel times along an arc $(i, j) \in A$ are non-negative integers denoted by τ_{ij} . The dynamic network $G_T = (N_T, A_T)$ is a time-expanded version of the static network for T periods (steps), where $N_T := \{i(t) \mid i \in N; t = 0, 1, \dots, T\}$. That is, each node in N corresponds to $T + 1$ nodes $i(t)$ in G_T , and the set A_T consists of movement arcs $A_M := \{(i(t), j(t + \tau_{ij})) \mid (i, j) \in A; t + \tau_{ij} \leq T; t = 0, 1, \dots, T\}$ and holdover arcs $A_S := \{(i(t), i(t + 1)) \mid i \in N; t = 0, 1, \dots, T - 1\}$.

The capacity of the arcs A_M at time t is $c_{ij}(t)$, while the capacity of the arcs A_S is equal to the node capacity $c_i(t)$. The number of people in node i at $t = 0$ is q_i . Capacities are defined as non-negative integers.

Let $x_{ij}(t)$ denote the flow that departs from node i at time t and reaches node j at time $t + \tau_{ij}$. The flow present in node i at time t (remaining units in that node at time $t - 1$) is denoted by $y_i(t)$.

The arc travel times and the number of time periods (steps) T are determined by the selected basic unit θ (the duration of a single step). The total number of periods T is obtained by dividing the evacuation time by θ . The choice of the basic unit θ is a compromise between the accuracy of the results and the computational complexity.

For illustration, a simplified layout of a shopping mall, as shown in Fig. 1, is used. It features four shops, each with a single door, a corridor, and two exits.

The corresponding static network (Fig. 2) has been constructed, with the corridor divided into three zones.

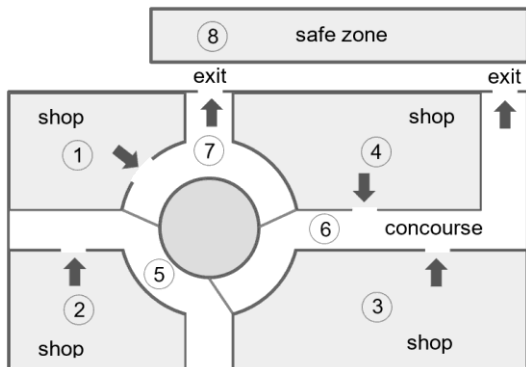


Fig. 1. Simplified building layout.

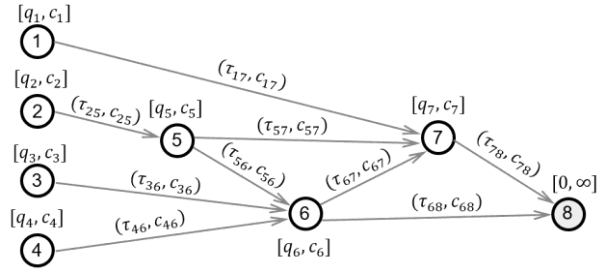


Fig. 2. Static network.

The network consists of eight nodes and nine arcs, where node 8 is the sink node, and the others are source nodes.

The dynamic network contains $T + 1$ copies of each source node and each sink node from the static network. A single super source and a single super sink node are added to it. The way the super source is connected to the actual source nodes depends on the specific problem being addressed. Dynamic flow problems can be treated as static flow problems within the dynamic network. In this framework, it is not necessary to assume that the input data remain constant over time. However, if this assumption holds, efficient solution algorithms can be utilized.

A. Average Evacuation Time Minimization Problem

Fig. 3 shows part of the dynamic network for this problem, based on the following input data: $\theta = 5$, $T = 5$;

- nodes

i	1	2	3	4	5	6	7	8
c_i	80	60	100	70	40	60	50	∞
q_i	50	20	60	10	20	30	25	0

- arcs

(i, j)	(1,7)	(2,5)	(3,6)	(4,6)	(5,6)	(5,7)	(6,7)	(6,8)	(7,8)
τ_{ij}	2	2	3	2	4	3	3	4	1
c_{ij}	15	15	15	15	15	15	15	15	15

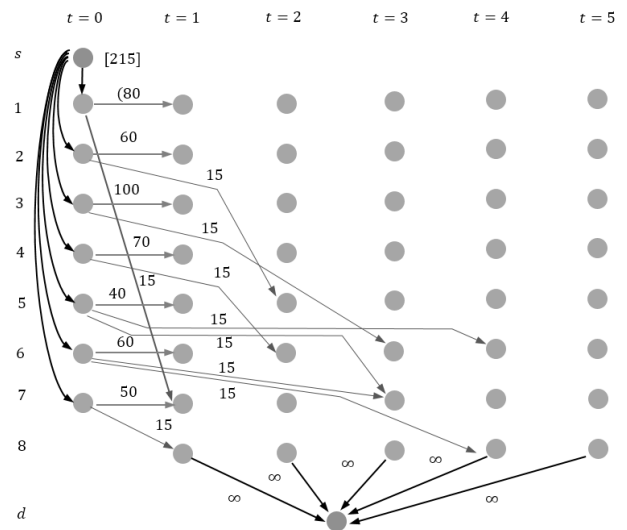


Fig. 3. Dynamic network.

The super source node s contains all the people in the building. Node s is connected only to the copies of the source nodes at $t = 0$. Arcs capacity is equal to the initial number of people in the respective nodes, i.e., $c_{s1} = 50, c_{s2} = 20$, and so on. All copies of the sink node d are connected to the super sink node d via arcs with infinite capacity. To avoid overcomplicating the figure, only the transition arcs $(i(0), j(\tau_{ij}))$, originating from nodes at $t = 0$, are shown. These arcs are repeated for $t = 1, 2, \dots, T - \tau_{ij}$, with capacities assigned according to the input data. Regarding holdover arcs, only those between the node copies at $t = 0$ and $t = 1$ are displayed; their capacity is equal to the respective node capacities. It should be noted that to solve the problem, the number of steps T must be significantly greater than 5. Furthermore, all node and arc copies that do not belong to any path between s and d are removed from the dynamic network.

Let $S \subset N$ be the set of source nodes in G , and $D \subset N$ be the set of sink nodes. The evacuation time for a given individual is equal to the time t at which they reach a node in D . This can be treated as the (turnstile) cost of the arcs $(i(t), d), i \in D; t = 1, 2, \dots, T$. Consequently, the average evacuation time is defined as:

$$\frac{\sum_{t=0}^T \sum_{i \in D} t x_{id}(t)}{\sum_{i \in S} q_i}$$

Since the denominator is constant, the formulation of the optimization problem, assuming constant input data (c_i, c_{ij}, τ_{ij}) , is as follows.

Find the minimum value of

$$Z = \sum_{t=0}^T \sum_{i \in D} t x_{id}(t), \quad (1)$$

subject to the following constraints:

$$x_{si}(0) = q_i, \forall i \in S \quad (2)$$

$$\sum_{t=0}^T \sum_{i \in D} x_{id}(t) = \sum_{j \in S} q_j \quad (3)$$

$$y_i(t+1) = y_i(t) + \sum_{k \in p(i)} x_{ki}(t - \tau_{ki}) - \sum_{j \in s(i)} x_{ij}(t) \quad (4)$$

$t = 0, 1, \dots, T; \forall i \in N$

$$y_i(0) = 0, \forall i \in N \quad (5)$$

$$y_i(t) = 0, \forall i \in D; t = 1, \dots, T$$

$$0 \leq y_i(t) \leq c_i, t = 1, \dots, T; i \in N - D; \quad (6)$$

$$0 \leq x_{ij}(t) \leq c_{ij}, t = 0, \dots, T - \tau_{ij}; \forall (i, j) \in A \quad (7)$$

where $p(i) := \{j \mid (j, i) \in A\}$ and $s(i) := \{j \mid (i, j) \in A\}$.

Constraints (4) define the net flow at the nodes of G_T , (5) impose restrictions on availability, while (6) and (7) represent the capacity constraints. To obtain the solution, any algorithm for the minimum cost flow problem is applied.

B. Maximum Dynamic Flow (MDF) Problem

This problem involves determining the maximum dynamic flow that reaches the sink node within a predefined number of steps (time horizon) T . In other words, it aims to determine the maximum number of people

who can be evacuated from a given building within a specified time. The problem can be solved by applying any of the algorithms for finding the maximum static flow from node s to node d in the dynamic network G_T . When constructing this network, it should be noted that the super source s is connected to all copies of all source nodes in G via arcs with infinite capacity and zero travel time. Furthermore, holdover arcs can be omitted, as it has been proven that they are not utilized by the flow [1]. The mathematical formulation for this setup is as follows.

Find the maximum value of

$$v(T) \quad (8)$$

subject to the following constraints:

$$\sum_{t=0}^T \sum_{i \in S} x_{si}(t) = v(T) \quad (9)$$

$$\sum_{j \in s(i)} x_{ij}(t) - \sum_{k \in p(i)} x_{ki}(t - \tau_{ki}) = 0 \quad (10)$$

$$t = 0, 1, \dots, T; i \neq s, d$$

$$\sum_{t=0}^T \sum_{i \in D} x_{id}(t) = v(T) \quad (11)$$

$$0 \leq x_{ij}(t) = c_{ij}, t = 0, \dots, T - \tau_{ij}; \forall (i, j) \in A \quad (12)$$

Solving the MDF problem using the G_T network is justified only if the capacities and travel times vary over time. However, if these remain constant, an efficient method exists for generating the MDF from a static flow [2]. This approach utilizes a network G with a single source node s and a single sink node d . If necessary, the network model of the building is brought into this form by adding a super source. The algorithm consists of the following steps:

1) Solve the problem of finding a static flow f from the source to the sink node of G that maximizes the linear function

$$(T+1)v - \sum_{(i,j) \in A} \tau_{ij} x_{ij} \quad (13)$$

subject to the following conditions:

$$\sum_{i \in N} x_{si} = v$$

$$\sum_{j \in s(i)} x_{ij} - \sum_{k \in p(i)} x_{ki} = 0, i \neq s, d \quad (14)$$

$$-\sum_{i \in N} x_{id} = -v$$

$$0 \leq x_{ij} = c_{ij} \quad (15)$$

This is essentially a minimum cost static flow problem. The maximum value of the function is equal to the magnitude of the MDF for T periods.

2) The MDF itself is found as follows:

- Decompose the static flow f with magnitude v into path flows between s and d . The following holds: $v = \sum_{i=1}^l v(P_i)$, where $v(P_i)$ is the magnitude of the flow along the i -th path.

- Each flow is repeated from $t = 0$ to $t = T + 1 - \tau(P_i)$, where $\tau(P_i)$ is the travel time along the i -th path (i.e., $v(P_i)$ units are sent at each step).

The dynamic flows obtained in this manner are called *temporally repeated flows* [1],[2].

Numerical analysis of the network from Fig. 2 shows that the magnitude of the MDF increases linearly for $T > 3$ by 30 units per step. This rate is determined by the total capacity of the arcs leading to node 8; thus, the throughput capacity of the building's exits is critical with respect to the maximum flow. It should be noted that this model assumes full utilization of each arc leading to the safe zone.

The MDF problem can be further refined to seek the maximum flow at each time step t . In this case, the objective function is redefined as $\sum_{t=1}^{T'} \sum_{i \in D} x_{id}(t)$, $\forall T' = 1, \dots, T$.

C. Quickest Flow (QF) Problem

In this problem, the objective is to minimize the time $T(v)$ required for a given number of initial occupants v to exit the building, i.e., the time in which a dynamic flow of a specified magnitude v travels from the source node s to the sink node d of the network. Net flow and arc capacity constraints apply. In a sense, the QF problem is the inverse of the MDF problem. It has been proven that the function $v(T)$, which defines the change in MDF, is monotonically increasing. The maximum increment Δv is equal to the maximum flow in the static network. Thus, to find $T(v)$ for a given v , one must find the smallest integer T such that $v(T) \geq v$. This can be achieved, for example, by using binary search.

Polynomial-time solution algorithms for the problem were proposed in [3]. In [4], the QF problem is solved by means of an optimization problem with a fractional objective function defined over the static network.

AGENT-BASED SIMULATION MODEL OF EVACUATION

The workspace in NetLogo is referred to as 'world'. It is composed of 'patches'. For this model, the size of a single patch is defined as 1 sq. m. The simulation progresses in intervals called 'ticks', which are assumed to have a duration of 1 second. Individual patches can represent: a wall, an obstacle, an exit, a safe zone, empty space (white), etc. These elements are used to construct the map of the world. Fig. 4 shows the map of simplified shopping center at a certain stage of the evacuation process.

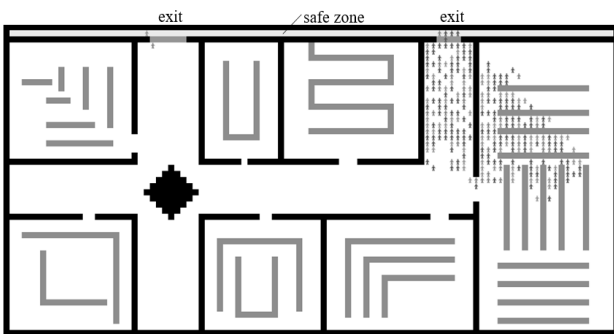


Fig. 4.

The model parameters are defined via a user interface and are categorized into two primary groups: initial state parameters and parameters influencing the evacuation process.

The initial state is determined by the number of occupants present in the shopping mall and their current positions within the facility at the onset of the evacuation. The occupancy count is treated as an input parameter, ranging from 40 to 3,800 individuals for this specific model. Their spatial distribution is generated randomly, following a uniform probability distribution.

Parameters affecting the evacuation process include individual movement speeds, the maximum occupancy density per "patch" (per sq. m), and the flow capacity of the exits. For this particular simulation experiment, the movement speed for all individuals within the shopping mall is fixed at 1 m/s.

The maximum number of people allowed in a single patch (per sq. m) is defined. This effectively sets the throughput capacity of the exits. This capacity is determined twice: first, by the number of patches when drawing the map, and second, by defining how many people can pass through one patch within 1 second.

In addition to input data, the interface dynamically displays real-time data regarding the evacuation process: the number of people remaining in the center at any given moment and the number of those who have reached the safe zone. The initial state of the population is generated first, and then the simulation begins.

The direction of movement for each individual is determined by a pre-generated distance map, which indicates the distance from every patch to the nearest exit. Fig. 5 shows the distance map of the modeled shopping center. Before taking each step, every person selects the adjacent patch with the smallest distance value to the exit. If multiple patches share the same minimum value, one is selected at random. A check is performed if the patch is 'free', meaning the occupancy limit has not been reached. If the patch is available, the person moves in that direction. However, if the patch is occupied, the other forward-facing patches (to the left and right of the chosen one) are checked; if any of them is free, the movement is redirected toward it. If all three patches are occupied, the individual waits for the current tick without moving.

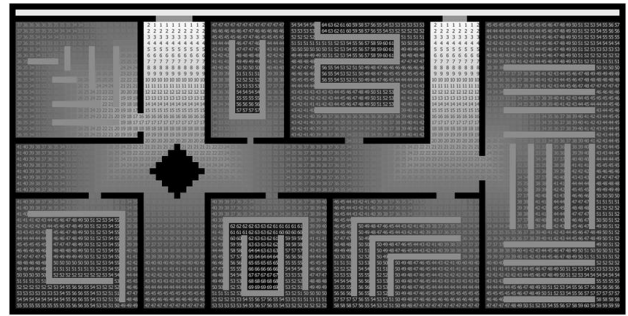


Fig. 5.

For this specific study, a 'world' with dimensions of 100 x 50 m was created. The layout of walls, obstacles, exits, and the safe zone is visible on the map on Fig. 4. A series of numerical experiments were conducted at two different exit throughput capacities: for the left exit- 6 persons per second and 2 persons per second; and for the right exit- 4

persons per second and 2 persons per second. For the first series of experiments, the total throughput capacity of both exits is 10 people per second, while for the second series, it is 4 people per second. Simulation ends when the last person leaves the building.

The performance measure is the evacuation completion time, i.e., the moment when the last visitor has left the shopping center. For each combination, ten experiments were conducted, the results were averaged and are shown in Fig. 6. The horizontal axis represents the average number of people at the initial moment of the simulation, while the vertical axis shows the seconds within which the evacuation process was completed.

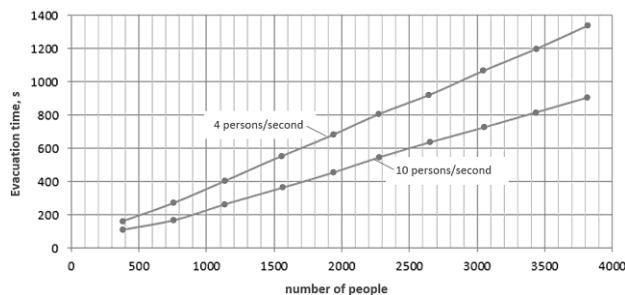


Fig. 6.

A small subset of the statistical data regarding the results obtained at an exit flow capacity of 10 people per second is presented in Table 1.

TABLE 1. STATISTICAL ANALYSIS OF EVACUATION TIME

Occupancy (Number of People)	Mean Value, s	Standard Deviation, s	Confidence Interval, s
750	175.4	6.52	± 3.79
1550	327.3	12.89	± 7.47
1950	448.2	10.52	± 6.1

The data in the table indicates that the dispersion around the calculated mean values is minimal, demonstrating that the obtained results are reliable for use as outcomes of the numerical experiment.

The first and most obvious conclusion is that the capacity of the exits significantly influences the evacuation time. The graph shows that the relationship between evacuation time and the number of people in the building is linear. Of particular interest is the zone between 400 and approximately 800 people at a throughput capacity of 10 people per second. It is evident that in this range, time increases considerably slower than it does for populations exceeding 800. This is due to the fact that when more than 800 people are in the shopping center, congestion begins to form at the exits (the right exit in Fig. 4). In other words, with fewer than 800 people in the building, the evacuation rate depends on the distances and the movement speed of the individuals, whereas at higher values, it is governed by the throughput capacity of the doors.

CONCLUSIONS AND FUTURE WORK

The process of building evacuation can be modeled through network problems, providing optimistic estimates of performance indicators. Given the structure of the static

network in building evacuation, its maximum flow-and consequently, the increase in maximum dynamic flow per period-is determined by the capacity of the exits.

Average Evacuation Time Minimization Problem is the most suitable for developing evacuation plans and conducting sensitivity analyses of the solution relative to the input data. This model accounts for the initial number of people and node capacities, allowing for the use of time-varying travel times and capacities throughout the process. It has been proven that the flow which minimizes the average evacuation time also maximizes the number of people reaching the safe zone at each time step and minimizes the total evacuation time [1].

Discrete mathematical models can be further refined. The area subject to evacuation can be divided into priority zones based on the level of threat. Arc travel times can be treated as a function of time and flow density.

To account for the influence of behavioral and organizational factors on the evacuation process, simulation models should be utilized. Current trends in the field involve the use of hybrid models, which simulate both the behavior of evacuees and concurrent physical processes, such as the spread of fire and smoke.

The simulation model presented here is relatively simple, yet even in this form, it can approximate the evacuation process and outline directions for its improvement. There are numerous opportunities for further developing the model. For instance, a hazard zone could be added that expands over time, blocking paths to specific exits, causing injuries to individuals, and slowing their movement. The behavior of individual agents is also subject to further refinement.

Numerous software products have been developed for solving evacuation problems, based on either mathematical or simulation models [5],[6].

ACKNOWLEDGEMENTS

We would like to express our gratitude to programme “Research, Innovation and Digitalisation for Smart Transformation” 2021-2027, funded by the European Union, Project BG16RFPR002-1.014-0008 “Sustainable development of Center for Competence “Quasar” for supporting this article.

REFERENCES

- [1] H. W. Hamacher and S. A. Tjandra, “Mathematical modelling of evacuation problems: A state of the art,” Fraunhofer ITWM, Kaiserslautern, Germany, Tech. Rep., 2001.
- [2] L. R. Ford and D. R. Fulkerson, *Flows in Networks*. Princeton, NJ: Princeton University Press, 1962.
- [3] R. E. Burkard, K. Dlaske, and B. Klinz, “The quickest flow problem,” *Methods and Models of Operations Research*, vol. 37, pp. 31–58, 1993.
- [4] P. Jaillet and L. Maokai, “On the quickest flow problem in dynamic networks: A parametric min-cost flow approach,” *Networks*, vol. 65, no. 2, pp. 123–138, 2015, <https://doi.org/10.1002/net.21574>.
- [5] E. D. Kuligowski and R. D. Peacock, *A Review of Building Evacuation Models*. Gaithersburg, MD: National Institute of Standards and Technology, 2005.

- [6] S. Casadesús-Pursals, F. Garriga, and M. Pujol, "Building evacuation: Principles for the analysis of basic structures through dynamic flow networks," *Journal of Industrial Engineering and Management*, vol. 6, no. 4, pp. 1081–1094, 2013, <https://doi.org/10.3926/jiem.805>.
- [7] L. G. Chalmet, R. L. Francis, and P. B. Saunders, "Network models for building evacuation," *Management Science*, vol. 28, no. 1, pp. 86–105, 1982, <https://doi.org/10.1287/mnsc.28.1.86>.
- [8] S. A. Tjandra and H. W. Hamacher, "Dynamic network optimization with application to evacuation problems," in *Operations Research Proceedings*, 2003, pp. 255–262.

Digital Sustainability: The Role of Smart HR Tools in Achieving Sustainable Development Goals (SDGs)

Stoyko Stoykov

*Vasil Levski National Military
University, Bulgaria*

stojkods@abv.bg

ORCID: [0000-0002-4885-713X](https://orcid.org/0000-0002-4885-713X)

Valentin Vasilev

*New Bulgarian University /NBU/,
Sofia, Bulgaria*

vvasilev@nbu.bg

ORCID: [0000-0002-0074-9578](https://orcid.org/0000-0002-0074-9578)

Gentian Koci

*Aleksandër Moisiu Universitet: Durrës,
Albania*

gentiankoci@aol.com

ORCID: [0009-0001-5369-4785](https://orcid.org/0009-0001-5369-4785)

Abstract: This chapter explores how digital transformation, smart HR tools, and AI-driven systems are reshaping Sustainable Human Resource Management (SHRM) and accelerating organizational progress toward the Sustainable Development Goals (SDGs). It argues that digital sustainability is not only a technological shift but a strategic framework that integrates automation, data analytics, digital communication, and intelligent HR platforms to reduce environmental impact, optimize workflows, and enhance the employee experience.

The chapter investigates how digital tools - such as AI-based recruitment, cloud HR systems, automated performance management, virtual collaboration platforms, and digital well-being applications - can lower the organizational carbon footprint by minimizing paper usage, reducing travel, and improving energy efficiency. These technologies also strengthen employee motivation, support flexible work models, and foster higher levels of engagement by enabling personalized learning, transparent communication, and more inclusive decision-making.

Particular attention is given to the delicate balance between technological efficiency and the "human factor," highlighting the importance of emotional intelligence, ethical AI, and human-centered digital design. Drawing on international studies and case evidence from European and Asian contexts, the chapter demonstrates how organizations that integrate both digital innovation and human values achieve more sustainable performance, stronger talent retention, and a healthier organizational culture.

Keywords: *Digital Transformation; Sustainable HRM; AI and Automation; Employee Motivation; SDGs.*

I. INTRODUCTION

Human resource management is changing as a result of the quick development of digital technology, automation, and artificial intelligence, making it crucial to accomplishing the global Sustainable Development Goals (SDGs). Digital HR technologies are now a strategic resource for environmental, social, and economic

sustainability rather than just a way to increase operational efficiency in the face of expanding competition, changing labor markets, and demands for organizational responsibility. Their responsibilities include process optimization, carbon footprint reduction, improving employee motivation and well-being, and creating an innovative and "green" engagement-focused culture. It is precisely for this reason that the study of digital transformation in Human Resource Management (HRM) and its contribution to the Sustainable Development Goals (SDGs) is emerging as a critical area for contemporary organizations and academic research.

This study applies a combined methodological approach, integrating elements of conceptual analysis and comparative review of good practices. The analysis is based on a review of relevant academic literature and secondary data related to the implementation of digital HR tools in various organizational and national contexts. The selected examples (e.g., Unilever, Siemens, IKEA, as well as practices from Estonia, Singapore, the Netherlands, Finland, and Canada) are used for illustrative and comparative purposes, rather than as a comprehensive empirical investigation.

II. DIGITAL HR TOOLS AS A DRIVER OF SUSTAINABLE DEVELOPMENT (SDGs)

The automation of processes and technologies based on artificial intelligence can bring benefits to numerous functions of public administration. Governments around the world are under pressure to operate more efficiently, deliver better services to citizens, and provide a more satisfying working environment for their employees. Lessons from the private sector show that large-scale automation has the potential to support the achievement of these goals. However, to reach this point, governments need to adopt a more strategic approach, embrace new technologies, and be prepared to act at scale. Process automation and AI-based technologies can benefit many

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.78>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

government functions, including significantly lower operating costs, more efficient processes, and reduced waste and errors (Gbr, R.A. and Abdullah, M.F., 2025).

The benefits of automation can be achieved relatively quickly. Many solutions can be built on existing IT systems without significant additional investment (Judijanto, L., 2025; Dolchinkov, N., 2025). The approach to deploying automation at scale is intuitive, starting with opportunity assessment, launching pilot projects, building the necessary infrastructure, and then scaling up (Serafimova, V., Dissanayake, H., Iddagoda, A., & Vasilev, V., 2025).

Establishing online procedures that allow citizens to submit applications and interact with service providers is already a major step forward for many administrations. In order to update internal operations and procedures and assist them in becoming essentially digital companies, the next step is to use automation at scale. Policies for human resource development must be completely in line with this change.

The reviewed international examples allow for the identification of both similarities and significant differences in approaches to digital HR transformation. In this context, it is important to emphasize that these practices should be interpreted critically, taking into account the specific institutional, cultural, and technological environments in which they are implemented. The comparative analysis indicates that successful models are characterized by the integration of technological solutions, organizational culture, and strategic management.

In turn, digital transformation in the field of human resources is becoming one of the most significant factors in achieving the Sustainable Development Goals (SDGs) formulated by the United Nations. Smart HR platforms, based on artificial intelligence, automation, and cloud solutions, not only optimize management processes but also create a new type of organizational sustainability, characterized by efficiency, transparency, and reduced resource consumption (Stefanova, D., Jaganjac, J., Vasilev, V., 2025; Chariatte, J., Asdourian, B., & Ingenhoff, D., 2026).

First, by automating and improving the objectivity of hiring, performance reviews, and career development, digital HR technologies help achieve SDG 8 (Decent Work and Economic Growth). More precision, fewer human errors, and more equitable judgments in human capital management are made possible by algorithmic selection and computerized competency monitoring systems.

Second, digitalization has a direct impact on SDG 13 (Climate Action). The transition to electronic documents, virtual training, online interviews, and remote work leads to a significant reduction in carbon emissions associated with transportation, office supplies, and energy consumption (Xu, L., De Vrieze, P., Lu, X., & Wang, W., 2022; Marinov, R., 2025). In this way, IT solutions become

a tool for environmental management, integrated within the framework of Strategic Human Resource Management (SHRM).

Third, through learning platforms, digital well-being programs, and engagement-tracking applications, HR departments contribute to SDG 4 (Quality Education) and SDG 3 (Good Health and Well-being). Digital solutions facilitate access to knowledge, create conditions for continuous learning, and support psychosocial well-being, especially in hybrid and remote work models (Toncheva-Zlatkova, V., 2025).

Lastly, SDG 5 (Gender Equality) is supported by the digital HR ecosystem through the use of algorithms for pay analysis, equal opportunity monitoring, and discrimination avoidance. In this approach, technologies support moral principles and an egalitarian culture in addition to automating procedures.

In conclusion, digital HR tools serve as a strategic catalyst for sustainable development. By combining the economic, social, and environmental facets of human capital management, they make Strategic Human Resource Management (SHRM) a crucial tool for organizational change that is in line with the SDG framework and international ESG regulations.

III. DIGITAL MOTIVATION AND WELL-BEING: USING TECHNOLOGY TO ENCOURAGE PARTICIPATION AND ECO-FRIENDLY PRACTICES

The potential of digital solutions in human resource management to serve as catalysts for sustainable behavior, organizational engagement, and intrinsic motivation is becoming more and more apparent. A new environment where employees receive quick feedback, individualized development possibilities, and instant access to support resources is created by digital engagement tools, well-being tracking programs, and online learning platforms. Work-life balance, emotional resilience, and increased trust between employees and the company are all directly supported by these processes.

A significant focus is the impact of digital tools on “green” behaviors within organizations. Through gamified systems, digital campaigns to reduce the carbon footprint, and automated messages promoting sustainable practices, HR departments effectively foster an ecological culture and collective responsibility. In this way, technologies not only enhance motivation but also broaden employee participation in sustainability initiatives, making environmentally responsible behavior an integral part of everyday organizational habits (Stefanova, D. P., Jaganjac, J., & Vasilev, V. P., 2026).

In addition, digital tools have the potential to support SDG 3 (Health and Well-being) and SDG 8 (Decent Work) through accessible mental health programs, digital consultations, and automated workload management systems. They help create an inclusive environment where

well-being is regarded as a strategic resource rather than a secondary concern (Bostancı, S., Vasilev, V., & Yıldırım, S., 2024). In this context, digital motivation becomes a key pillar for achieving sustainable HR policies.

*A. Technology and Humanity in Balance:
Behavioral, Cultural, and Ethical Aspects*

Sustainable human resource management necessitates careful evaluation of the balance between technical efficiency and human sensitivity, notwithstanding the substantial advantages of digitalization (Stefanova, D., Popescu, C., Vasilev, V., 2026; Mohammadian, B., 2025). Maintaining a corporate culture built on ethics, empathy, and trust depends on this equilibrium. According to Kandpal, V., Tyagi, V., & Kaur, H. (2022), excessive automation can result in alienation, diminished autonomy, and a loss of belonging, all of which have a detrimental impact on motivation and engagement. Thus, rather than taking the role of human connection, contemporary HR technology must be built to enhance it.

The SDGs, especially SDG 5 (Gender Equality) and SDG 10 (Reduced Inequalities), place a strong emphasis on the ethical implications of AI and automation. Algorithmic decision-making needs to be open, auditable, and devoid of biased trends. Otherwise, rather than reducing social inequality, technologies run the risk of perpetuating it. Here, HR specialists are responsible for upholding moral norms, keeping an eye out for data biases, and maintaining human oversight over important hiring decisions (Bartekova, M., & Janikovicova, S., 2025; Adewumi, A. S., Opoku, A., & Dangana, Z., 2024).

From a cultural standpoint, emotional intelligence in management is made possible by striking a balance between technology and human contact. Effective communication, empathy, and trust-building skills become critical success factors in hybrid and digital work environments (Gigauri, I., Vasilev, V., & Sidova, D., 2025). By ensuring that digital tools serve as partners rather than replacements, a human-centered approach promotes sustainable organizational development and enhances the organization's overall ESG profile.

*B. Examples of Digital Sustainability in HRM in
Practice and Their Strategic Aspects*

Finding pertinent examples that demonstrate the efficacy of suggested practices is closely related to the search for long-term solutions for the successful creation and use of human resource policies in any firm. In order to show readers the wide range of applications of AI in human resource development, the authors describe three areas of application: business, the public sector, and the security sector.

Examples from Organizations in the Business Sector

✓ Unilever - AI systems for sustainable talent management. Unilever implements integrated AI platforms that automate key recruitment processes pre-screening

interviews, competency analysis, and gamified psychometric assessments. This approach minimizes physical travel and paperwork, thereby reducing the carbon footprint and improving HR process efficiency. Beyond the environmental impact, digitalization ensures greater objectivity, supports equality policies, and promotes an inclusive organizational culture.

✓ Siemens - Digital Learning Ecosystem for Green Competencies

Siemens has developed global AI-based adaptive learning modules through which employees build expertise in areas such as energy efficiency, sustainable technologies, and eco-friendly production. These digital learning programs significantly reduce the need for physical infrastructure, business travel, and localized training, thereby supporting SDG 4 (Quality Education), SDG 9 (Industry, Innovation, and Infrastructure), and SDG 13 (Climate Action). HR analytics enable precise competency management and support long-term talent retention.

✓ IKEA - Digital Tools for Well-being and Sustainable Behavior. In order to promote work-life balance, IKEA uses platforms and applications to track employee engagement, emotional climate, and well-being. In addition, the organization uses interactive ads, waste reduction programs, and integrated digital challenges to encourage sustainable behavior. This strategy improves motivation, links technology solutions with the "human factor," and aids the organization in achieving a number of important SDGs (Yao, J., Zhang, Y., Sun, Y., et al., 2025).

C. Examples from Public Sector Organizations

✓ Estonia - Sustainable Human Resource Management and the Digital State

With more than 99% of public services available online, Estonia is a global leader in e-governance. The way public administration manages its human resources has been drastically changed by this paradigm. SDG 16 (Peace, Justice, and Strong Institutions) and SDG 12 (Responsible Consumption and Production) are supported by the e-HRM platform, which reduces administrative burden, lowers material resource costs, and facilitates all processes—from hiring and appointments to performance evaluation. Additionally, improved labor forecasts, optimal employment planning, and enhanced civil service efficiency are made possible by digital tools.

✓ Singapore - Smart Nation and Digital HR Solutions for Sustainable Management

Singapore uses cutting-edge HR technology as part of the Smart Nation program, such as virtual learning platforms, AI-assisted hiring tools, and analytical models for competency management in public administration. Adaptive training programs are used by public institutions to help staff members acquire digital and green capabilities, which are critical for sustainable development (Mishra,

R.K., Kumari, C.L., Janaki Krishna, P.S., & Dubey, A., 2022). These technologies promote energy efficiency, lessen the need for in-person training and business travel, and establish a flexible work style that has been shown to improve engagement and well-being. SDGs 4 (Quality Education), 11 (Sustainable Cities and Communities), and 9 (Industry, Innovation, and Infrastructure) are all in line with this practice.

✓ Netherlands - Digital Administration and HR Ecosystem Focused on Well-being and Sustainability. The Netherlands is creating a government HR ecosystem that incorporates digital technologies for career management, human resource planning, and skills evaluation. Platforms like Rijkscloud make it possible to manage training and development centrally, maximize interagency mobility, and improve public sector appointment transparency. Digital technologies that track stress and strain, a crucial component of sustainable public employee management, lay a major emphasis on well-being. In line with SDGs 8 (Decent Work and Economic Growth), 16 (Peace, Justice, and Strong Institutions), and 13 (Climate Action), the Dutch model incorporates sustainable policies into HR operations by fusing technical efficiency with a human-centered approach.

D. Examples from the Security Sector

✓ Finland - Digital Training and Sustainable Management in Defense

The Finnish Armed Forces use integrated digital HR systems for training management, competency evaluation, and workforce planning. The carbon footprint is decreased by reducing the requirement for physical training grounds and real-world resources with virtual simulators and e-learning platforms. In line with SDGs 3 (Good Health and Well-Being), 9 (Industry, Innovation, and Infrastructure), and 12 (Responsible Consumption and Production), digital solutions also facilitate accurate workload forecasting and promote the welfare of military personnel.

✓ Canada - Police Services and AI for Sustainability and Efficient Workforce Management. Digital HR platforms, such as AI-based scheduling systems that optimize work hours, lower the risk of occupational burnout, and improve safety through appropriate resource allocation, are used by Canadian police departments. Digital psychometric tools for hiring and employee evaluation promote career advancement and foster openness, both of which are essential for fostering public trust. In keeping with SDGs 8 (Decent Work and Economic Growth) and 16 (Peace, Justice, and Strong Institutions), these solutions enhance institutional sustainability.

✓ Singapore - Intelligent Systems for Training and Risk Management in the Security Sector. Singapore's Ministry of Defence and public security agencies utilize advanced intelligent systems for planning, risk forecasting, and training through VR/AR technologies. These innovations significantly reduce the need for physical infrastructure,

optimize personnel training, and enable operations that previously required substantial resources. Integrated HR platforms provide a unified competency framework, facilitating workforce mobility and sustainable skills development. These practices directly contribute to SDG 4 (Quality Education) and SDG 11 (Sustainable Cities and Communities).

Particular attention should be given to the link between digital HR tools and secure system design. In the context of increasing digitalization, human resource management increasingly involves the processing of sensitive personal data, requiring a high level of data protection and regulatory compliance. Key aspects include cybersecurity, algorithmic transparency, and the ethical use of artificial intelligence. The existence of clear policies and risk management mechanisms is essential for building trust and ensuring organizational resilience.

For the purposes of this study, it is important to clearly distinguish between digital transformation as a broad strategic process, the digitalization of human resource management functions, referring to the implementation of specific technological tools, and sustainability outcomes, which reflect the long-term impact on organizational development. This distinction allows for a more precise analysis of the interconnections between technology, management practices, and sustainable results.

IV. CONCLUSIONS AND APPLICABILITY IN A BROADER ORGANIZATIONAL CONTEXT

The examples demonstrate that digital HR tools function as a bridge between technological transformation and sustainable organizational development. Their practices show that:

✓ Both the social and environmental aspects of sustainability are concurrently supported by digitalization. Employee health and well-being are enhanced, expenses are decreased, and the carbon footprint is minimized through automation, online learning, and HR analytics.

✓ The tools foster high levels of organizational engagement, trust, and inclusion. AI objectivity, data transparency, and personalized development enhance motivation and talent retention across all types of organizations (Vasilev, V. P., Efremovski, I. P., & Gigauri, Z., 2026).

✓ These approaches are fully applicable in both the public sector and the security sector. Both the public sector and the security sector may fully utilize them. Digital HR solutions in public administration can help achieve SDG 16 (Effective Institutions) by optimizing recruiting, increasing transparency, lowering administrative load, and guaranteeing equal access to career advancement. Digital tools in the security sector can improve psychological resilience and well-being, optimize human resource allocation, maintain personnel readiness through adaptive training modules, and improve training reliability - all

important aspects for organizations with strategic functions (Marinov, R., Stoykov, S., & Marinov, P., 2019).

✓ Digital HR solutions have global applicability, regardless of organizational size or sector. Technological platforms can be implemented in multinational corporations, small businesses, universities, government institutions, and public security structures alike (Stanković, J.J., Östh, J., & Marjanović, I., 2026). This makes digitalization a universal tool for achieving the SDGs.

V. CONCLUSION

Digital HR tools, whether in the private sector, public administration, or the security sector, demonstrate strong applicability for achieving sustainable development. They support:

✓ Resource Optimization - Automation and digitalization reduce costs, accelerate processes, and minimize the environmental footprint.

✓ Improving Motivation and Well-Being - Digital learning tools, flexible scheduling, and workload monitoring systems raise employee happiness and work quality.

✓ Increasing Transparency and Institutional Trust - Equal access to job prospects, transparent evaluation standards, and moral management are all made possible by electronic HR systems, which are essential components of contemporary public institutions and security services.

✓ Supporting SDGs in a Broad Context - Technologies accelerate the achievement of goals such as SDG 8 (Decent Work and Economic Growth), SDG 9 (Industry, Innovation, and Infrastructure), SDG 12 (Responsible Consumption and Production), SDG 13 (Climate Action), and SDG 16 (Peace, Justice, and Strong Institutions).

The analysis demonstrates that the successful implementation of digital HR solutions requires not only technological readiness but also an integrated approach that combines organizational culture, leadership, and strategic risk management. In this sense, organizational sustainability should be understood as the result of a balanced interaction between digital transformation and the socio-ethical dimensions of human resource management.

In this sense, digital transformation in HRM is not merely a modern trend but a strategic tool for building efficient, sustainable, and adaptive organizations - whether operating in business, public administration, or the security sector.

REFERENCES

- [1] Adewumi, A. S., A. Opoku, and Z. Dangana (2024). Sustainability Assessment Frameworks for Delivering Environmental, Social, and Governance (ESG) Targets: A Case of Building Research Establishment Environmental Assessment Method (BREEAM) UK New Construction; Corporate Social Responsibility and Environmental Management 31: 1. <https://doi.org/10.1002/csr.2768>.
- [2] Bartekova, M. & Janikovicova, S. (2025). Sustainable Development of Women Entrepreneurship in Selected Central European Countries. In I. Gigauri (Ed.), Sustainable Entrepreneurship and Family Business for Women's Empowerment (pp. 41-68). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-8694-1.ch003>
- [3] Bostanci, S., Vasilev, V., & Yildirim, S. (2024). Strategies and Policies in Recycling Food Waste: The Intermediary Role of Municipalities. Journal of Recycling Economy & Sustainability Policy, 3(2), 160–167. Retrieved from <https://respjournal.com/index.php/pub/article/view/56>
- [4] Chariatte, J., Asdourian, B. & Ingenhoff, D. (2026). Digital place branding through sustainability: how cities and regions of the world gain visibility through climate change solutions. Place Brand Public Dipl ; <https://doi.org/10.1057/s41254-025-00409-1>
- [5] Dolchinkov, N. (2025). Radioactive waste storage as an element of national security. (2025). ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the International Scientific and Practical Conference, 5, 81-87. <https://doi.org/10.17770/etr2025vol5.8502>
- [6] Gbr, R.A. and Abdullah, M.F. (2025). Enabling Green HRM Through Digital HR Transformation: Practical Insights and Future Strategies from UST University. Journal of Science and Technology. 30, 7 (Jul. 2025). DOI:<https://doi.org/10.20428/jst.v30i7.2957>
- [7] Gigauri, I., Vasilev, V., & Sidova, D. (2025). The Role of Leadership and Corporate Social Responsibility for Sustainable Entrepreneurship: Good Practices From Georgia and Bulgaria. In I. Gigauri (Ed.), Sustainable Entrepreneurship and Family Business for Women's Empowerment (pp. 165-176). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-8694-1.ch008>
- [8] Judijanto, L.(2025). Reconfiguring HR Roles for Sustainability Governance: A Bibliometric View of Strategic Role Transformation, West Science Social and Humanities Studies, 3(09), pp. 1277–1286. <https://doi.org/10.58812/wsshs.v3i09.2263>.
- [9] Kandpal, V., Tyagi, V., Kaur, H. (2022). Smart City: Sustainable City for Tackling Urban Challenges. In: Jadhav, P., Choudhury, R.N. (eds) Infrastructure Planning and Management in India. Studies in Infrastructure and Control. Springer, Singapore. https://doi.org/10.1007/978-981-16-8837-9_8
- [10] Marinov, R. (2025). The dynamics of military security – challenges and forecasts in the conditions of global (IN)SECURITY. (2025). ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the International Scientific and Practical Conference, 5, 163-170. <https://doi.org/10.17770/etr2025vol5.8467>
- [11] Marinov, R., S. Stoykov and P. Marinov (2019). Urbanized Territories Non-Existing Part of Crisis Response Operations; 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), Sandanski, Bulgaria, 2019, pp. 1-4, <https://doi.org/10.1109/CREBUS.2019.8840084>
- [12] Mishra, R.K., Kumari, C.L., Janaki Krishna, P.S., Dubey, A. (2022). Smart Cities for Sustainable Development: An Overview. In: Mishra, R.K., Kumari, C.L., Chachra, S., Krishna, P.S.J., Dubey, A., Singh, R.B. (eds) Smart Cities for Sustainable Development. Advances in Geographical and Environmental Sciences. Springer, Singapore. https://doi.org/10.1007/978-981-16-7410-5_1
- [13] Mohammadian, B. (2025). Responsible Behavior Design and Sustainable Future. In: Panait, M., Gigauri, I., Raimi, L. (eds) Sustainable Economic Development. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-96224-0_10
- [14] Serafimova, V., Dissanayake, H., Iddagoda, A., & Vasilev, V. (2025). Inclusive Leadership and Corporate Social Responsibility for Women's Empowerment: From Good Ideas to Sustainable Solution. In I. Gigauri (Ed.), Sustainable Entrepreneurship and Family Business for Women's Empowerment (pp. 177-202). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-8694-1.ch009>

- [15] Stanković, J.J., Östh, J., Marjanović, I. (2026). Benchmarking Local Government Smart City Initiatives: A Data Envelopment Analysis of European Urban Centers. In: Džunić, M., Östh, J., Muratori, S. (eds) *Advancing Urban and Local Governance in Western and Transition Europe. Local and Urban Governance*. Springer, Cham. https://doi.org/10.1007/978-3-032-04265-1_7
- [16] Stefanova, D. P., Jaganjac, J., & Vasilev, V. P. (2026). Strategic Communications for Climate Resilience: European Goals, Local Policies, and Best Practices. In S. Bostanci, S. Yildirim, & V. Vasilev (Eds.), *Empowering Resilient Communities Through Climate Action, Renewable Energy, and Waste Management* (pp. 19-38). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3373-0862-3.ch002>
- [17] Stefanova, D., Jaganjac, J., Vasilev, V. (2025). On the Road to Sustainability: How Storytelling Changes Public Management and Leads to Motivation and Organizational Development. In: Panait, M., Gigauri, I., Raimi, L. (eds) *Sustainable Economic Development*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-96224-0_3
- [18] Toncheva-Zlatkova, V. (2025) Serving beyond duty: the social responsibility in public administration; <https://doi.org/10.37075/JOMSA.2025.2.07>, *Journal of Management Sciences and Applications*, 4(2), pp. 247–261. Available at: <https://www.jomsa.science/index.php/jomsa/article/view/137>
- [19] Vasilev, V. P., Efremovski, I. P., & Gigauri, Z. (2026). Sustainable Human Resource Management and Development Through Innovative Approaches and Practices. In A. Wojcik-Czerniawska (Ed.), *Exploring Human Resource Innovations in E-Economy* (pp. 461-474). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3373-4307-5.ch017>
- [20] Stefanova, D., Popescu, C., Vasilev, V. (2026). Green Transition and Human Resource Management–Sustainable Development Through Effective Management of Green Collar Workers. In: Malik, F.A., Kushwah, S.V., Aslam, M.S., Reyed, R.M., Haghi, A.K. (eds) *Aligning ESG Goals with the UNs Sustainable Development Goals Planning*. World Sustainability Series. Springer, Cham. https://doi.org/10.1007/978-3-032-01715-4_14
- [21] Xu, L., De Vrieze, P., Lu, X., & Wang, W. (2022). Digital twins approach for sustainable industry. In Paper presented at *Advanced Information Systems Engineering Workshops*, Leuven, Belgium. https://doi.org/10.1007/978-3-031-07478-3_11.
- [22] Yao, J., Zhang, Y., Sun, Y. et al. (2025). Study based on managerial compensation incentives and analyst attention perspectives of corporate digital transformation and sustainability performance. *Sci Rep* 15, 37290 <https://doi.org/10.1038/s41598-025-21194-0>

Why Economic Security is National Security. Economic Determinism in the U.S. National Security Strategy 2025

Svetoslav Velkov

Department for National and International Security
University of Library Studies and Information Technologies
Sofia, Bulgaria
s.velkov@unibit.bg

Abstract—The text analyzes the fundamental link between economic stability and national security, focusing on the 2025 U.S.¹ National Security Strategy. This strategy reaffirms the view that the economy is the foundation of power and that military superiority is impossible without a strong industrial base, technological innovation, and energy independence. Furthermore, it posits that economic sovereignty and the well-being of the American middle class are key to the nation's global influence and prosperity. The evolution of this concept is examined from the Reagan era to the present, highlighting the transition from globalism to economic nationalism under the "America First" motto.

Keywords—economic security, national security, strategy, economic security strategy, national security strategy, national economic interests, industrial base, protectionism

I. INTRODUCTION

A broad national security strategy is the course of action adopted following an assessment of the strategic environment. A widely cited understanding within academia posits that "the Strategic Concept aims to provide a consensual basis for the nation's objectives, priorities, instruments, and means within the politico-military context it will navigate over the next five to ten years. It may operate under various designations, such as national security strategy or concept, security and defense concept, or security and defense policy. What they all share is that in the contemporary world, the concept of defense is evolving and has become integrated into a broader concept of security" (van Eekelen, Willem F., 2010, p. 3). According to the U.S. Department of Defense Dictionary of Military and Associated Terms, a National

Security Strategy is "A document approved by the President of the United States for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to national security" (Dictionary of Military and Associated Terms, 2021, p. 156). Consequently, the National Security Strategy of a modern state constitutes a dynamic equation designed to ensure coherence between desired objectives and available resources by employing the most effective course of action.

II. THEORETICAL FRAMEWORKS AND CONTEMPORARY DIMENSIONS OF THE SECURITIZATION OF THE ECONOMY

Representatives of the Copenhagen School, whose works have profoundly influenced security theory and practice, propose a comprehensive understanding of security and its strategic management. Barry Buzan and Lene Hansen conceptualize security strategy as a process of securitization and desecuritization. They advocate the foundational premise that national security is intrinsically linked to the state's capacity to continue functioning, as well as the resilience of society in the face of changes and threats. In this context, a Security Strategy represents the formulation of policies to manage the internal and external environment to avert or mitigate threats while preserving the core elements of the state and society (Buzan, Barry, & Hansen, Lene, 2009). Buzan's concept expands the traditional, force-centric understanding of security, demanding that strategy encompass measures across five primary security sectors: military, political, economic, societal, and environmental. Therefore, a National Security Strategy must be multisectoral, addressing all five

¹ U.S. - United States [of America]

domains rather than focusing exclusively on military aspects.

Stephen M. Walt, an authoritative American foreign policy and national security expert renowned for his work in international relations theory and strategic analysis, outlines a distinct vision. He defines National Security Strategy as a framework for aligning available means with established ends. It must explicitly articulate the state's core interests, the threats arrayed against them, and the actions—predominantly political and military, but also economic—that will be undertaken to protect these interests, maximizing advantages while minimizing vulnerabilities (Walt, Stephen M., 2005). The approach adopted by Walt and other strategic analysts (often reflecting the Classical Strategic Triangle model) dictates that a strategy must incorporate the following components:

- Ends: What the state seeks to achieve and protect (national interests, fundamental values).
- Ways: How the state will achieve its objectives (political, military, economic, and diplomatic instruments).
- Means: The resources the state possesses to execute the ways (capabilities, budgets, human resources, alliances).

According to this model, the National Security Strategy represents a dynamic equation that must ensure alignment between desired objectives and available resources by applying the most effective course of action.

Evidently, economic issues are an inextricable component of any National Security Strategy. Consequently, Robert Gilpin, a leading scholar in international political economy, focuses specifically on economic security, defining its essence, scope, and strategic application. His approach is pivotal for understanding the nexus between economic realities and national security strategy. Economic security, according to Gilpin, is a state's ability to pursue its national economic interests—including economic prosperity, sustainable growth, and control over strategic resources—without being vulnerable to coercion or significant disruption by other states or non-state actors. Thus, an economic and national security strategy must aim to minimize external dependencies that could be leveraged against the state (Gilpin, R., 2003).

Susan Strange, another preeminent scholar of international political economy, emphasizes that structural power (the power to shape the rules of the game) is key to understanding the intersection of security and economics. In this context, her conception of state economic security involves freedom from the threat of severe economic

damage, whether originating from natural forces, market dynamics, or the actions of hostile states and corporations. This necessitates an economic security strategy directed toward exercising power to shape the economic environment to the state's advantage—i.e., manipulating the foundational structures of the global economy that determine who wins and who loses. Strange's approach is broader than the traditional view, requiring economic security strategy to focus not merely on defense, but on actively shaping the global environment. Therefore, it must encompass elements related to control over four structural domains: the knowledge structure, the financial structure, the security structure, and the production structure (Strange, Susan, 1996).

The EU² Economic Security Strategy establishes the framework for current EU policy in this domain. This document delineates the EU's transition from a purely economic union to a geopolitical actor that places security at the core of its economic policy. "Security is a concept that has new and multiple dimensions. One of them is economic security. Economic security is vital to Europe's prosperity and its ability to shape the future... The EU's strategy must focus on mitigating risks, promoting competitiveness, and building partnerships to strengthen our economic security without seeking self-sufficiency" (European Economic Security Strategy, 2023).

According to the publication Policy Recommendations for U.S. Economic Security, economic security encompasses elements of the economy that influence stability, technological competitiveness, and resilience, each of which empowers the U.S. government to better protect national security and assert its international influence. "Sound economic security policies can help the United States prevent, mitigate, and recover from risks and shocks, such as wars, cyberattacks, pandemics, and natural disasters. To design effective economic security measures, U.S. policymakers must collaborate closely with the private sector to develop a shared understanding of risks and tailor appropriate solutions and strategies" (Policy Recommendations for U.S. Economic Security, 2025).

Consequently, "within the entire construct of national security, a distinct place belongs to economic security. Experience demonstrates that only a high level of economic security can serve as a guarantor of any country's sovereignty and independence, and as a guarantor of its stable and sustainable socio-economic development" (Velkova, L., 2015).

III. ECONOMICIZATION - THE NEW PARADIGM IN THE AMERICAN SECURITY STRATEGY

The strategic documents adopted in 2025, including the new National Security Strategy of the United States of America, evidence the new approach of President D.

² EU - European Union

Trump's administration toward national security. Economic security, social protection, and the self-actualization of the nation's populace—underpinned by the "America First" principle—dictate a heightened focus on the economic aspects of national security. The diverse instruments employed to strengthen the country's industrial base are necessitated by a qualitatively new stage of interdependence and competition among global economic actors, encompassing trade, investment, technology, finance, and domestic economic regulation.

The United States reaffirms and will enforce the Monroe Doctrine to restore American preeminence in the Western Hemisphere. It declares intent to undertake targeted missions to secure the border and dismantle cartels, including the use of "lethal force" where necessary, to replace the failed, exclusively law-enforcement-based strategy of the past several decades.

Following a prolonged period of liberalization in the international exchange of goods and services, the Trump presidency is characterized by a shift toward protectionism, driven by the perception that the American market is "too open" to trading partners, constituting a "threat to national security." The guiding U.S. foreign policy principle of "America First" underscores priorities for managing economic competition with China. The Strategy frames China primarily as an economic challenge, stating that Washington will rebalance its economic relationship with Beijing by prioritizing reciprocity and fairness to restore American economic independence.

This period is marked by the tightening of foreign trade controls concurrently with the deregulation of the domestic economy, the activation of mechanisms to stimulate entrepreneurship, and the provision of financial and economic incentives to corporate and individual entities in the interest of economic and social security.

Economic growth is viewed as the primary engine of public welfare, and tax mechanisms are to be utilized to stimulate business activity and increase Americans' disposable income. This is grounded in the understanding that a nation unable to protect prosperity at home cannot project and protect its interests abroad. Utilizing systemic, historical, and comparative analysis of priority objectives across various periods of U.S. development allows us to identify the Trump administration's specific approaches in the current era of geopolitical, economic, and technological challenges. The reconceptualization of the role of the economy and economic policy within the national security strategy—and the provision of population welfare through the defense of the American way of life, compared to the approaches of previous presidential administrations—has today become one of the core principles of U.S. state strategy in the Trump era: "Economic security is national security."

The U.S. National Security Strategy specifically emphasizes the role of American economic power in national security, the nation's capacity to manufacture requisite products and systems, defense capabilities, and societal well-being. Underscoring the significance of this core principle in U.S. policy and the interconnectedness of economic and military security, Peter Navarro, Donald Trump's trade and manufacturing policy advisor during his first term, noted: "Only through American prosperity will there be the growth, resources, and technological innovations for the most advanced military force in the world" (Navarro, Peter, 2018).

National security issues have traditionally occupied a prominent place in U.S. presidential addresses. A pivotal milestone in documenting national policy priorities and identifying primary security threats was the National Security Act of 1947. Since 1950, the President of the United States was mandated to present an annual report to Congress outlining the goals and objectives of the nation's national security policy, identifying critical problems requiring resolution, and proposing the methods and means to address them (The National Security Act, 1947). The Goldwater-Nichols Department of Defense Reorganization Act of October 4, 1986, mandated the annual submission of this document; however, this requirement was subsequently modified, and the report is now presented less frequently.

IV. ECONOMIC NATIONALISM AS A SECURITY DOCTRINE

Comparing the approaches of previous presidential administrations to national security issues, P. Navarro observes that during the Reagan era, the prevailing concept was achieving peace exclusively through strength, with this strength focused on military power—"comprehensive and technologically innovative military dominance on land, at sea, in the air, and, of course, in the realm of 'Star Wars'" (Navarro, Peter, 2018).

During Ronald Reagan's presidency, the Strategy was promulgated twice. In 1987, alongside the aforementioned issues, a dedicated section addressed the U.S. position in the global economy, the international financial system, and the promotion of regional and global free trade agreements.

The 1987 U.S. National Security Strategy, presented by the Reagan administration, is a historical document that established the tradition of regularly publishing such reports. In it, the economy is not merely an adjunct but a fundamental pillar of national power within the context of the Cold War. The Reagan administration emphasized that U.S. security depends directly on the vitality of the American economy. A strong dollar and low inflation were viewed as instruments for projecting influence. The document argued that only a growing market economy could sustain the high defense expenditures necessary to

deter the Soviet Union. Therefore, the Strategy championed "economic freedom" as an ideological counterpoint to communism and demonstrated the transition to "Peace through Strength," where economic superiority was deemed as vital as the nuclear arsenal (National Security Strategy of the United States of America, 1987).

In February 2015, U.S. President Barack Obama presented another National Security Strategy to Congress, reflecting the strategic vision of the then-Democratic administration regarding the contemporary world order and the U.S. role within it. This strategy was a product of continuity, built upon the framework formulated in 2010. The Democratic government's successes were presented as a vector for the country's further development, resulting more in an adaptation of Obama's initial 2010 strategy to the changing international environment than an entirely new strategic vision. It was dedicated to the concept of national renewal and the restoration of U.S. global leadership by strengthening the foundations of American power and global influence. Thus, Obama embedded into the core of the National Security Strategy all the primary priorities of the concept of domestic strength as the bedrock of global influence: a robust economy, accessible education and healthcare, energy security, and innovation (National Security Strategy of the United States of America, 2015).

The 2017 National Security Strategy, during D. Trump's first term, identified four vital national interests: 1. Protect the American people, the homeland, and the American way of life. 2. Promote American prosperity. 3. Preserve peace through strength. 4. Advance American influence (National Security Strategy of the United States of America, 2017).

The 2022 U.S. National Security Strategy, adopted under the Biden administration, placed economic aspects at the heart of its vision, framing them as an instrument for domestic renewal and geopolitical competition against authoritarian regimes, primarily China and Russia. The foundational economic pillars of this strategy included:

1. Investing in National Power (First at Home): The strategy explicitly states that domestic economic strength is a prerequisite for global leadership. This approach, termed "Bottom-up and middle-out," entails:

a) Modern Industrial Strategy: Unlike previous periods that relied heavily on the free market, the 2022 Strategy calls for strategic public investments in key sectors.

b) CHIPS³ and Science Act & Inflation Reduction Act (IRA): These major legislative initiatives are cited as tools to build a resilient and modern U.S. industrial base,

particularly in critical and emerging technologies like microelectronics, advanced computing, and biotechnology.

c) Strengthening the Middle Class: Economic prosperity is viewed as a driver of democratic vitality and societal cohesion, both critical for national security.

2. Shaping the Rules of the Global Economy: The U.S. seeks to work with allies and partners to establish 21st-century economic rules to ensure they serve democratic values and open markets rather than autocracies, through:

a) Technology Governance and Standards: The focus is on shaping global standards for critical technologies (AI⁴, 5G/6G, cyber) and utilizing export controls (e.g., on microchips) to restrict adversaries' access to foundational American technologies.

b) Addressing Economic Coercion: The Strategy calls for building collective capacity to counter economic coercion (e.g., China's weaponization of trade).

c) Integrating Economics and Security: Economic policy is tightly integrated with foreign and security policy, viewing trade and investment through the prism of "democracies versus autocracies."

3. Securing Resilient Supply Chains: The Biden administration placed a strong emphasis on supply chain resilience, employing a multilateral approach, in contrast to the unilateral approach of the 2017 Trump Strategy:

a) Partnership and Diversification: The objective was to reduce reliance on single sources (especially China) for critical goods through cooperation with trusted allies (e.g., via the Indo-Pacific Economic Framework - IPEF).

b) Climate as an Economic Threat: Climate change was explicitly identified as a transnational threat with direct economic consequences—from impacts on agriculture and infrastructure to energy security. Investments in clean energy are viewed as a tool for economic advantage and security.

Despite elements of continuity, the new U.S. National Security Strategy (2025) stands in stark contrast to the last 30 years of American policy, transitioning from ideological interventionism and competition to prioritizing economic relations. While previous administrations assessed national security threats and economic challenges discretely, under both the first and second Trump presidencies, these are approached holistically. The trade practices of other nations are viewed as being just as dangerous to the United States as their military capabilities.

³ CHIPS - Creating Helpful Incentives to Produce Semiconductors

⁴ AI - Artificial Intelligence

This approach led to the recognition of the inadequacy of market mechanisms—which ostensibly should guarantee the nation's economic security and strengthen the U.S. global position—and the necessity of introducing measures to support domestic producers, shield the domestic market from foreign competition, and mitigate the risks of dependence on imported finished goods and raw materials.

Based on the premise that the United States is "too open" to its trading partners, with whom it is engaged in fierce economic competition, unprecedented measures were enacted to protect the domestic market from foreign economic actors—both private and state-owned. At the presidential level, investigations were initiated into the U.S. economy's reliance on imports of steel, aluminum, and other rare metals and products. Based on findings that American manufacturers had suffered substantial injury from these imports, significant tariffs were imposed.

The new National Security Strategy reaffirms the fundamental principle that economic strength is foundational to U.S. national security. It explicitly states that the greatest U.S. asset is its highly developed, dynamic, and innovative economy, serving as the bedrock of the American way of life. This necessitates stimulating new waves of American investment in the domestic economy. It underscores that domestic economic vitality, competitiveness, and prosperity are the vectors of American power and global influence, achieved through building the most robust industrial base in the world, capable of meeting production needs in both peacetime and wartime (specifically the defense-industrial base). The development of the most reliable and innovative energy sector is presented as a prerequisite for the U.S. remaining a net energy exporter, which is critical for economic growth and global leverage.

Addressing and identifying unfair trade practices, intellectual property theft, and state-directed subsidies are framed as threats to the American economy and national security. The U.S. National Security Strategy elevates economic power as the foundation of security, directly linking national security to economic growth spurred by reindustrialization and deregulation in the energy sector.

Strengthening the industrial base and supply chain resilience of the U.S. manufacturing and defense sectors—particularly regarding semiconductors, critical minerals, and dual-use technologies—is tied to the identification of an extensive list of risks. These include the reliance of the national industry and the U.S. defense sector on imports of specific raw materials, rare-earth metals, and certain types of equipment and technologies (e.g., between 2013 and 2016, imports from China accounted for 78% of all rare-earth materials imported into the U.S. (Assessing and Strengthening the Manufacturing and Defense Industrial

Base and Supply Chain Resiliency of the United States, 2018)).

In this manner, the Strategy formalizes the growing role of economic security as a central organizing principle of foreign policy, including the use of export controls and investment restrictions as national security instruments. The document diverges from the traditional internationalist consensus and repudiates "globalism" and "so-called free trade," which have "hollowed out" the American middle class and industrial base. It also envisions the utilization of tariffs to encourage the re-shoring of critical manufacturing.

The importance of America's technological edge in leading and critical technologies is identified as a vital priority for ensuring future economic and military dominance. Technological competition is viewed primarily as a struggle for power and security, rather than merely an economic issue. The focus is on preserving U.S. technological superiority, particularly in dual-use technologies such as AI, quantum technologies, and supercomputing. In this context, restrictions on the transfer of advanced technologies to adversary nations are mandated, and the imperative to protect critical economic infrastructure, including cybersecurity, is a pervasive theme requiring specialized attention.

The Strategy is distinguished by a revision of global economic relations and the consolidation of an approach rooted in economic nationalism and conditional hegemonism. Leveraging U.S. financial and technological advantages to build coalitions and shape 21st-century rules across all spheres of the global economy aims to achieve freer and fairer conditions for global trade through bilateral diplomacy. This often involves the threat of tariff measures to address trade imbalances and counter "predatory trade," intellectual property theft, and cyber espionage, especially from China. Emphasis is placed on conditional support for allies in Europe, urging them to assume greater responsibility for their own defense and eliminate mercantilism overcapacity, while simultaneously opening their markets to American goods and services. These aspects demonstrate a fundamental realignment toward "America First," where domestic economic flourishing is viewed as a direct and indispensable precondition for U.S. national security and global power.

V. CONCLUSION

The approach of the current U.S. presidential administration toward national security is characterized by a strong economic focus as the foundation for prosperity and the reinforcement of the country's global posture. While the 2017 U.S. National Security Strategy initiated the reorientation toward an "America First" economy, the 2025 National Security Strategy deepens and radicalizes this approach, making economic self-sufficiency and

sovereignty the central and nearly exclusive pillar of national security. This entails a narrower definition of the national economic interest, a profound emphasis on fortifying the American economy, and a geographic pivot toward the immediate U.S. neighborhood. Consequently, the new philosophy embedded in the December 2025 U.S. National Security Strategy validates the necessity of fully integrating economic security into national security.

REFERENCES

- [1] Dr. Willem F. van Eekelen, The Definition of a National Strategic Concept, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, 2010. [Online]. Available: <https://www.dcaf.ch/sites/default/files/publications/documents/WIM%2520Nepal%2520DCAF%2520Strategic%2520Concept%2520low.pdf>
- [2] U.S. Department of Defense (DoD) Dictionary of Military and Associated Terms, November 2021. [Online]. Available: <https://irp.fas.org>, [Accessed March 25, 2026], <https://irp.fas.org/doddir/dod/dictionary.pdf>
- [3] Buzan, Barry, Lene Hansen. The Evolution of International Security Studies. Cambridge University Press, 2009. [Online]. Available: IR101, <https://ir101.co.uk>, [Accessed March 25, 2026], <https://ir101.co.uk/wp-content/uploads/2018/10/buzan-the-evolution-of-international-security-studies-compressed.pdf>
- [4] Walt, Stephen M. Taming American Power: The Global Response to U.S. Primacy. W. W. Norton & Company, 2005. [Online]. Available: The Belfer Center for Science and International Affairs, <https://www.belfercenter.org>, [Accessed March 25, 2026], <https://www.belfercenter.org/publication/taming-american-power-global-response-us-primacy>
- [5] Gilpin R., Globalna politicheska ikonomiya. Razbirane na mezhdunarodniya ikonomicheski red, Izd. "Damyan Yakov", S., 2003.
- [6] Strange, Susan. The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge University Press, 1996. [Online]. Available: PagePlace, <https://api.pageplace.de>, [Accessed March 25, 2026], https://api.pageplace.de/preview/DT0400.9780511837340_A23680086/preview-9780511837340_A23680086.pdf
- [7] Evropeyska strategiya za ikonomicheska sigurnost“ (COM (2023) 360 final), 2023. [Online]. Available: European Commission, https://commission.europa.eu/index_en, [Accessed March 25, 2026], https://ec.europa.eu/commission/presscorner/detail/bg/ip_23_3358
- [8] Policy Recommendations for U.S. Economic Security, February 2025, ITI, Promoting Innovation Worldwide, [Online]. Available: ITIC, <https://www.itic.org>, [Accessed March 25, 2026], https://www.itic.org/documents/general/ITI_Economic-Security-Recommendations_022425FINAL.pdf
- [9] Velkova L., Koruptsiyata – zaplaha za ikonomicheskata sigurnost, Izd. „DioMira“, S., 2015, s. 142. ISBN 978-954-2977-22-3
- [10] National Security Strategy of the United States of America, Washington, the White House, November 2025. [Online]. Available: [The White House](https://www.whitehouse.gov), <https://www.whitehouse.gov>, [Accessed March 25, 2026], <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>
- [11] Navarro Peter, Why Economic Security Is National Security. White House. December 10 2018. [Online]. Available: RealClearPolitics, <https://www.realclearpolitics.com>, [Accessed March 25, 2026], https://www.realclearpolitics.com/articles/2018/12/09/why_economic_security_is_national_security_138875.html
- [12] The National Security Act of 1947 – July 26, 1947. [Online]. Available: Oxford University Press, <https://global.oup.com>, [Accessed March 25, 2026], <https://global.oup.com/us/companion.websites/9780195385168/resources/chapter10/nsa/nsa.pdf>
- [13] National Security Strategy of the United States of America, Washington, the White House, January, 1987. [Online]. Available: Historical Office of the Secretary of War, <https://history.defense.gov/>, [Accessed March 25, 2026], <https://history.defense.gov/Portals/70/Documents/nss/nss1987.pdf?ver=FUZbPLy3ZDfa4UTDpMkNzw%3D%3D>
- [14] National Security Strategy of the United States of America, Washington, the White House, February, 2015. [Online]. Available: The White House, President Barack Obama, <https://obamawhitehouse.archives.gov>, [Accessed March 25, 2026], https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf
- [15] National Security Strategy of the United States of America, Washington, the White House, December 2017. [Online]. Available: The White House, President Donald J. Trump, <https://trumpwhitehouse.archives.gov>, [Accessed March 25, 2026], <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
- [16] National Security Strategy of the United States of America, Washington, the White House, October 2022. [Online]. Available: The White House, President Joe Biden, <https://bidenwhitehouse.archives.gov>, [Accessed March 25, 2026], <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>
- [17] Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, September 2018. [Online]. Available: The Department of War, <https://media.defense.gov>, [Accessed March 25, 2026], <https://media.defense.gov/2018/oct/05/2002048904/-1/-1/1/assessing-and-strengthening-the-manufacturing-and%20defense-industrial-base-and-supply-chain-resiliency.pdf>

Vulnerability Assessment of Wild Medicinal and Aromatic Plants Along the Bulgarian Black Sea Coast Using Rapid GIS-Based Model

Stoyan Vergiev

Department of Ecology and Environmental Protection
Technical University of Varna
Varna, Bulgaria
stvergiev@gmail.com

Abstract—The Bulgarian Black Sea coast is characterised by a high and specific biodiversity, acting as a critical conservation area for species within both the Balkan Peninsula and Europe. Wild medicinal and aromatic plants represent not only a vital ecological resource but also a significant Bulgarian export. Despite existing regulatory frameworks, the uncontrolled harvesting of non-protected species and species with conservation status exceeding permitted quotas persists. The combination of these practices and anthropogenic pressure, results in cumulative negative impacts on habitats, loss of localities, depletion of communities, and substantial long-term economic consequences. The Bulgarian strategy for the sustainable use of biological resources is based on the rigorous assessment and monitoring of the distribution, abundance, and population dynamics of wild species. Constantly changing market demands for specific quantities and types of medicinal plants, alongside evolving negative anthropogenic factors, require deploying dynamic, GIS-based Rapid Model for Vulnerability Assessment of Medicinal Plants (RMVAMP). The aim of the present study is to conduct a vulnerability assessment of wild medicinal and aromatic plants along the Bulgarian Black Sea Coast. By incorporating objective criteria and weighted values within a GIS environment, natural localities and habitats along the Bulgarian Black Sea Coast were classified according to their degree of vulnerability and are visualised using a colour scale on a specialised map. High-vulnerable areas were identified, where the medicinal plant harvesting requires stricter regulation. The species analysis effectively identifies and categorised species in three groups: resilient, vulnerable, and highly vulnerable. The species identified as most vulnerable to overharvesting include *Pancreaticum maritimum* L., *Leucojum aestivum* L., *Orchis morio* L., *Orchis purpurea* Huds., *Paonia peregrina* Mill., *Platanthera bifolia* (L.) L. C. Rich., *Ruscus aculeatus* L., *Ruta graveolens* L., and *Ephedra distachya* L.

Keywords— Medicinal Plants, Eastern Bulgaria, Bulgarian Black Sea Coast, Vulnerability Assessment.

I. INTRODUCTION

Over the last decade, Bulgaria has faced a marked transition in the utilization of medicinal plants, as traditional harvesting for personal use is increasingly supplanted by large-scale commercial extraction for export [1], [2]. The increasing demand for raw materials within the pharmaceutical and cosmetic industries, combined with a drive for rapid economic returns, has placed natural populations under significant anthropogenic impact [3]. Despite existing regulatory frameworks, illegal harvesting and the systematic exceeding of quotas remain critical challenges that threaten Bulgaria's biodiversity, which is a key renewable resource [4].

Illicit harvesting, combined with extensive and regional-scale anthropogenic stressors, exerts a cumulative negative impact on natural habitats [2], [5]. In accordance with established scientific frameworks for the sustainable management of Bulgaria's bioresources, comprehensive monitoring of the occurrence, abundance, and population fluctuations of wild species is essential to ensure long-term resource sustainability [4], [6], [7]. Effective bioresource management relies on high-quality quantitative data, obtained from long-term studies of exploitation pressures. As environmental and market conditions evolve, the development of adaptive models becomes crucial for the spatial-temporal evaluation of vulnerability in medicinal and aromatic plants [4].

The Bulgarian Black Sea coast represents a heterogeneous mosaic of ecosystems and is characterised by a high and specific biodiversity. The coastal area acts as a critical conservation area for species within both the Balkan Peninsula and Europe and provides habitats and critical refuges for a variety of rare medicinal and aromatic taxa that are increasingly pressed by intensive tourism and rapid urbanization [4]. Implementation of models along the entire coastal area facilitates the identification of critical

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.148>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](#).

“hotspots” where biodiversity is affected by unregulated harvesting and habitat degradation.

One of the most established global scale tools for analysing and assessing the overexploitation of medicinal plants is the Rapid Vulnerability Assessment (RVA), which has been validated and tested in series of studies [8] - [11]. Modern conservation strategies require enhancing and expanding this model in order to incorporate not only species-specific assessments but also a holistic analysis of entire communities and habitats. Unlike the RVA model, its adaptation, the “Rapid Vulnerability Assessment Model for Medicinal Plants” (RMVAMP) [4], [5], [12] relies on a combination of additional criteria to better prioritise of conservation zones on regional and local scale. Well-defined criteria, integrated within a GIS environment enable dynamic scaled assessments and habitat mapping based on extensive datasets [4], [5], [13].

The aim of the present study is: 1) to conduct a vulnerability assessment of wild medicinal and aromatic plants along the Bulgarian Black Sea Coast, 2) to classify natural localities and habitats according to their degree of vulnerability, visualised using a colour scale on a specialised map, 3) to identify high-vulnerable areas where medicinal plant harvesting requires stricter regulation.

II. MATERIAL AND METHODS

The Bulgarian Black Sea coast is characterised by a unique climatic transition from temperate continental to sub-Mediterranean conditions from north to south. The strong maritime influence causes milder winters and specific humidity levels, favouring the spread of rare medicinal and aromatic plants [14]. The northern Dobrudja Plateau is dominated by intensive agriculture, leaving wild medicinal plants confined to fragmented steppe habitats and field margins. In contrast, the southern reaches around Burgas and the Strandzha massif are defined by extensive forests and higher humidity, supporting a greater density of woodland species. The investigated area faces rapid urban overdevelopment and infrastructure expansion. This coastal sprawl is the primary driver of habitat fragmentation, necessitating urgent spatial management to protect both rare and common plant populations [4], [5], [13].

To map the study area, five-step GIS workflow that integrated field data with spatial modelling tools was developed (Fig. 1). The Input Data phase integrated heterogeneous datasets, including biodiversity inventory based on existing literature records, historical distribution data [15], [16], [17], and precise GPS coordinates collected during field surveys and remote sensing methods covering the vegetation periods from 2008 to 2024. These inputs were processed to generate Species Distribution Vector Polygons, delineating the precise spatial boundaries of each target taxon.

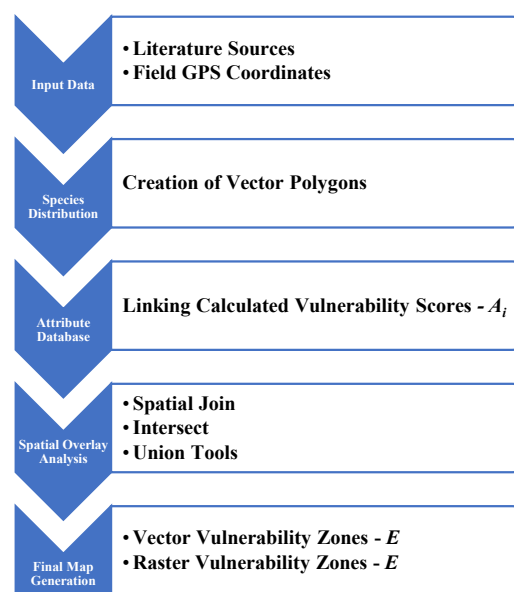


Fig. 1. Methodological GIS workflow diagram of the RMVAMP framework for spatial vulnerability assessment.

Attribute Tables were constructed and linked to the vector geometry, populating the database with the calculated integral vulnerability scores (A_i) for each species.

Conservation status, as well as endemic and relics designations, were determined after [16], [18]. The international conservation status of taxa was determined based on Annexes II and V of Directive 92/43/EEC (Habitats Directive), Annex I of the Bern Convention, and Annex II of the CITES Convention (the Convention on International Trade in Endangered Species).

A regional-level plant species assessment scheme based on the Rapid Vulnerability Assessment (RVA) method [8] - [11], [19], [20], modified by Vergiev [4], [5] was applied. The model includes two main groups of criteria: biological (distribution and conservation status) and socioeconomic factors. The vulnerability of each taxon is determined by ten predictors, each assessed on a point scale from 0 (not applicable) to ascending values reflecting an increasing degree of threat.

The integral score for each taxon is calculated as a weighted sum of the values for the ten criteria. The mathematical model applies specific weighting coefficients to the points awarded for each parameter according to the following formula:

$$A_i = \sum_{j=1}^{10} w_j \cdot C_{ji} \quad (1)$$

where,

A_i – general vulnerability assessment of the taxon i

w_j – coefficients of significance of the criterion j (shown in Table 1)

C_{ji} – estimate score of criterion j for taxon i .

TABLE 1 SUMMARY SCHEME OF CRITERIA FOR THE ASSESSMENT OF
 PLANT TAXA MODIFIED AFTER [4], [5], [21], [22].

Code	Criterion	
<i>Coefficients</i>	<i>Predictors</i>	<i>Score</i>
C1	Presence and distribution of the species in floristic regions and subregions of Bulgaria	
0.50	Only in the study region	5
	From 2 to 15 regions	1
	From 16 to 29 regions	0
C2	Population fragmentation	
0.50	Highly fragmented	5
	Low fragmented	3
	Unfragmented	0
C3	National conservation status (Included in the Bulgarian Biological Diversity Act)	
1.25	Included in Annex 2	3
	Included in Annex 3	3
	Included in Annex 4	2
	Not included	0
C4	Red Data Book Criterion	
1.00	CR Critically Endangere	4
	EN Endangered	3
	VU Vulnerable	2
	NT Nearly Endangered	1
	LC Low Affected	0
	DD/NE, Insufficient Data, Not Rated	0
	N/A	0
C5	Endemics and Relics	
1.25	Endemic to Bulgaria	5
	Endemic to Bolcan Peninsula	3
	Relics	2
	N/A	0
C6	International conservation status criterion	
1.25	IUCN	2
	Directive 92/43/EEC	2
	Berne Convention	2
	CITES	2
	N/A	0
C7	Plant parts used	
2.00	Whole plants	4
	Roots, rhizome	3
	Flower, seed, and inflorescence	2
	Leaves	1
C8	Resource origin	
0.50	Only from wild	4
	Wild and trial cultivation	3
	Wild and small-scale cultivation	2
	Only from cultivation	1
C9	User group	
0.50	Local people, local exchange and trade	4
	Local people and trade	3
	Local people and local exchange	2
	Local people	1
C10	Life forms	
2.00	Long lived perennial	4
	Short lived perennial	3
	Biennial	2
	Annual	1

A spatial Overlay Analysis was performed using the Spatial Join and Intersect/Union tools to merge overlapping species polygons and calculate cumulative environmental pressure [12].

The workflow concluded with the Generation of the Final Vulnerability Map, producing a high-resolution vector/raster output that delineates and categorises the specific geographic zones based on their cumulative vulnerability index (E).

The final vulnerability assessment of a specific territory (E) shifts the focus from a simple species count to a spatial perspective, recognising that site vulnerability depends on both species richness and individual taxon sensitivity. It is calculated using the following formula:

$$E = \frac{\sum_{k=1}^n A_k}{n} \quad (2)$$

where,

E – general vulnerability assessment of the territory

A – vulnerability assessment of each individual taxon k

n – total number of assessed taxa in the territory.

For map drawing, the following were used: UTM Zone 35 North map projection, WGS84 terrestrial coordinate system and the Baltic altitude system.

The reliability of the RMVAMP model was tested by conducting field checks across 15 randomly selected high-vulnerability zones. At each validation site, empirical field observations were conducted to assess actual habitat degradation, signs of overexploitation, and current anthropogenic pressure. These field-based metrics were then statistically compared with the model's predictive outputs, confirming a high degree of correlation between the theoretical vulnerability index (E) and the real-world anthropogenic impacts observed on the ground.

III. RESULTS AND DISCUSSION

A total number of 1846 plant species were recorded in the region is. This relatively compact territory accounts for 45.4% of all vascular plant life in Bulgaria. According to Medicinal Plants Act of the Republic of Bulgaria and subordinate legislation, 591 of these species were recognised as medical and aromatic plants and were subsequently assessed. This number is 32% of all inventoried species. Fifty-five species are assessed with high conservation status.

The Rapid Vulnerability Assessment (RVA) approach is based on the notion that a limited number of factors have a decisive influence on the sustainable use of medicinal plants. Typically, this assessment is calculated by summing 5 to 7 predictors, which allows for the rapid identification of species threatened by overexploitation. However, when a comprehensive analysis of a specific area is required, and not just individual taxa, simple summary of data is insufficient.

The RMVAMP model operates on the 80/20 Principle, recognising that a handful of critical factors often drive most ecological outcomes [23]. The model shifts the focus from a simple tally of species to a more spatial perspective, and the vulnerability of a specific site is more than just the sum of its plants. This represents a significant upgrade from the original RVA.

Unlike classical methods, the Rapid Vulnerability Assessment Model for Medicinal Plants (RMVAMP) builds on this model by integrating additional aspects and critical factors that directly affect the resources in the given area.

The predictors are structured into two main groups. The first covers ecological criteria, such as distribution, habitat fragmentation, and conservation status. Distribution is assessed according to the presence of the species in the different floristic regions of Bulgaria, based on the hypothesis that widespread taxa are more resilient. The degree of fragmentation of populations serves as an indicator of their ability to recover. Conservation status integrates four criteria (national and international), with the accumulation of protective categories increasing the vulnerability index.

The integration of high-weight predictors, such as the specific plant parts used (C7, weight 2.00) and life forms (C10, weight 2.00), ensured that the analysis was highly sensitive to the intrinsic biological capacity of the species to recover from harvesting stress. The extraction of roots and rhizomes, as well as whole plant harvesting is more invasive than that of foliage and other vegetative organs. Species that are obtained only from the wild or are used by a wide range of users are classified as more endangered. The assessment is based on a detailed inventory of the flora in the study area, compiled from literary sources and the author's field studies. The second group deals with socioeconomic status.

Although the model is aimed at identifying the vulnerability of individual locations, it can also be applied to identify the vulnerability of individual species. Based on the quantitative index scores (A_i), the 591 assessed species were successfully categorized into distinct vulnerability classes:

1) Vulnerable species: *Sedum acre* L. *Artemisia alba* Turra, *Helichrysum arenarium* (L.) Moench, *Galium odoratum* (L.) Scop., *Echinops sphaerocephalus* L., *Galanthus nivalis* L., *Glaucium flavum* Crantz, *Asarum europaeum* L., *Valeriana officinalis* L., *Convallaria majalis* L., *Cercis siliquastrum* L., *Frangula alnus* Mill., *Lilium martagon* L.

2) Highly vulnerable species: *Pancreatium maritimum* L., *Primula veris* L., *Carlina acanthifolia* All., *Paeonia peregrina* Mill., *Asparagus officinalis* L., *Berberis vulgaris* L., *Alchemilla vulgaris* L., *Leucojum aestivum* L., *Ephedra distachya* L., *Ruscus aculeatus* L., *Orchis morio* L., *Orchis purpurea* Huds., *Orchis simia* L., *Cyclamen coum* Mill., *Artemisia lerchiana* Weber, *Platanthera bifolia* (L.) L. C. Rich., *Ruta graveolens* L.

Cumulative weighted values were incorporated in GIS environment. The natural habitats in the Bulgarian Black Sea Coast were categorised into classes of vulnerability and were indicated on the created map using colour scale (Fig. 2).

Applying the constructed model and as a result of the "overlay" analysis, all values within the areas of overlap of the polygons were summarised and 53 zones of high vulnerability were identified.

The identification of areas with a degree of vulnerability is only the first step in a long and tough process of protecting the habitats of medicinal and aromatic plants. Our role as scientists is to investigate and to analyse, followed by prioritizing and using limited resources for the protection of medicinal plants. This should be accompanied by the implementation of the entire set of regulatory documents and punitive instruments for the preservation of natural habitats. In my opinion, educational initiatives are also extremely important to inform about the available medicinal plants in each area, along with small projects for the protection and expansion of habitats.

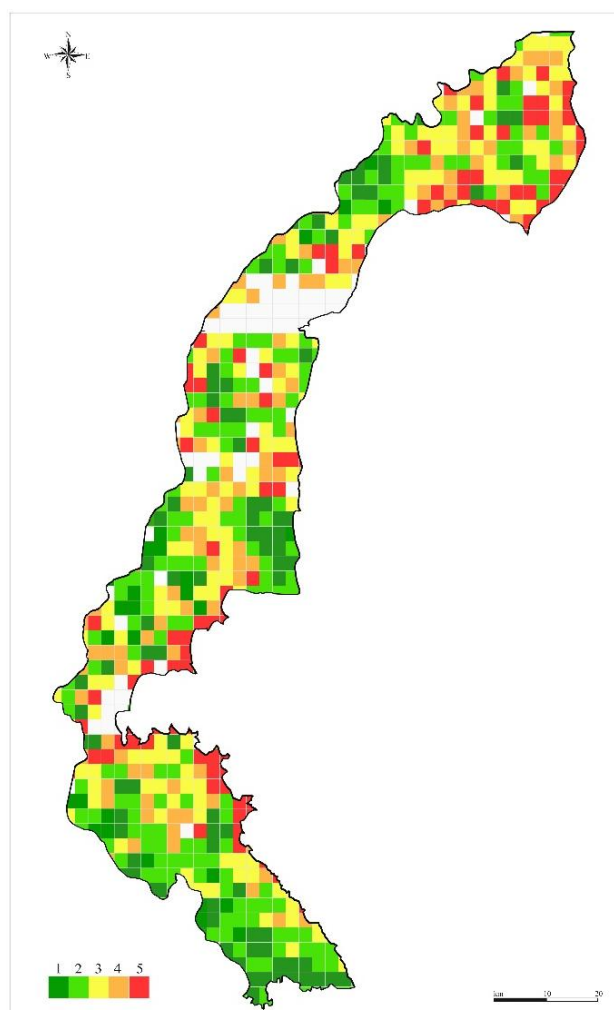


Fig. 2. Vulnerability assessment of medicinal plants. From 1 – non vulnerable to 5 – highly vulnerable. White cells represents urbanised territories.

The practical utility of the RMVAMP framework lies in its ability to provide environmental managers and authorities with actionable spatial data. Traditional conservation plans often apply broad regional restrictions that can be economically inefficient and difficult to enforce. By contrast, the pinpoint accuracy of the 53 identified hotspots allows the Bulgarian Ministry of Environment and Water to deploy targeted conservation measures.

In these critical zones, we recommend the immediate implementation of temporary harvesting bans (quotas set to zero) for highly vulnerable species, paired with strict spatial monitoring during the peak vegetative and collecting seasons. To alleviate the pressure on wild populations within these hotspots, regional economic programs should incentivize small-scale, local cultivation initiatives (shifting species scores from 4 to 1 on the C8 resource origin scale). Ultimately, balancing scientific spatial modelling with strict legislative enforcement and community-based conservation projects offers the most viable path toward the sustainable management of Bulgaria's wild medicinal bioresources.

IV. CONCLUSIONS

This study demonstrates the application and theoretical framework of the GIS-based Rapid Model for Vulnerability Assessment of Medicinal Plants (RMVAMP) along the Bulgarian Black Sea Coast. By combining multi-criteria ecological and socioeconomic factors into a weighted mathematical matrix, the model successfully shifts resource evaluation from simple species counts to a dynamic spatial analysis. Cumulative assignment in more predictors defines species as more vulnerable.

The established total number of plant species found in the region is 1846. This relatively compact territory accounts for 45.4% of all vascular plant life in Bulgaria. According to Medicinal Plants Act of the Republic of Bulgaria and subordinate legislation, 591 of them were recognised as medical and aromatic plants and were assessed. This number is 32% of all inventoried species.

Cumulative weighted values were incorporated in GIS environment. The natural habitats in the Bulgarian Black Sea Coast were categorised into classes of vulnerability and were indicated on map using colour scale.

The present study validated the practical value of the framework, successfully delineating 53 high-vulnerability hotspots that require immediate regulatory intervention and stricter harvesting quotas. Future research will expand this GIS-driven workflow to cover the remaining northern and southern segments of the Bulgarian coast, establishing a unified spatial database for bioresource preservation.

REFERENCES

- [1] R. Sharma, S. Kaur, and S. Kr. Uniyal, (2022), Population and vulnerability assessment of high value medicinal plants in the Alpine regions of western Himalaya, *J Appl Res Med Aromat Plants*, Vol. 26, 100353, <https://doi.org/10.1016/j.jarmap.2021.100353>.
- [2] L. Evstatieva, R. Hardalova, and K. Stoyanova, (2007), Medicinal plants in Bulgaria: diversity, legislation, conservation and trade, *Phytol. Balcan.*, vol. 3, no. 3, pp. 415-427, 2007.
- [3] A.C. Hamilton, (2004), Medicinal plants, conservation and livelihoods, *Biodiversity and Conservation*, 13, 1477-1517, <https://doi.org/10.1023/B:BIOC.0000021333.23413.42>
- [4] S. Vergiev, (2025), Rapid GIS-based model for vulnerability assessment of medicinal plants: a case study of the Varna District (North-eastern Bulgaria), *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, 1, 589-593, <https://doi.org/10.17770/etr2025vol1.8698>
- [5] S. Vergiev, (2016), Theoretical aspects of rapid GIS-based model for vulnerability assessment of medicinal plants in Bulgaria, *Proceedings of Fifth International Conference Geographical Sciences and Education*, November 4-5, 2016, Shumen, Bulgaria.
- [6] G. A. Boot, and R. E. Gullison, (1995), Approaches to developing sustainable extraction systems for tropical forest products, *Ecological Applications*, vol. 5, no. 4, pp. 896-903, 1995. <https://doi.org/10.2307/2269340>
- [7] K. Gould, A. F. Howard, and G. Rodríguez, (1998), Sustainable production of non-timber forest products: natural dye extraction from El Cruce Dos Aguadas, Petén, Guatemala, *For. Ecol. Manag.*, vol. 111, no. 1, pp. 69-82, 1998. [https://doi.org/10.1016/S0378-1127\(98\)00309-0](https://doi.org/10.1016/S0378-1127(98)00309-0)
- [8] A. B. Cunningham, (1996), People, park and plant use: Recommendations for multiple-use zones and development alternatives around Bwindi Impenetrable National Park, Uganda, *People and Plants Working Paper*, vol. 4, 58, UNESCO, Paris.
- [9] A. B. Cunningham, (1992), Development of a conservation policy on commercially exploited medicinal plants: a case study from southern Africa," in *Conservation of Medicinal Plants. Proceedings of an International Consultation*. Cambridge University Press. Cambridge, UK, <https://doi.org/10.1017/CBO9780511753312>
- [10] A. B. Cunningham, (1994), Integrating local plant resources and habitat management, *Biodivers Conserv*, vol. 3, pp. 104-115, 1994. <https://doi.org/10.1007/BF02291880>
- [11] A. Cunningham, (2001), *Applied Ethnobotany: People, Wild Plant Use & Conservation*: London, EarthscanUK & Sterling.
- [12] S. Narayan, R. Nicholls, E. Trifonova, M. Filipova-Marinova, I. Kotsev, S. Vergiev, S. Hanson, D. Clarke, (2012), Coastal habitats within flood risk assessments: role of the 2D SPR approach, *Coastal Engineering Proceedings*, 1(33) management.12, pp. 1-9, 2012. <https://doi.org/10.9753/icce.v33.management.12>
- [13] S. Vergiev, (2018), GIS mapping of plant biodiversity hotspots in the Bulgarian Floristic region Black Sea Coast, *SocioBrains*, vol. 52, pp. 172-178. 2018.
- [14] I. Kopravlev, (2002), *Geography of Bulgaria*. Sofia: ForKom.
- [15] B. Kitanov, (1976), *Vegetation*. Sofia: Prof. M. Drinov Acad. Publ.
- [16] B. Asyov, A. Petrova, D. Dimitrov, R. Vasilev, (2012), *Conspectus of the Bulgarian vascular flora. Distribution maps and floristic elements*. Sofia: Bulgarian Biodiversity Foundation.
- [17] I. Bondev, (1991), *Vegetation of Bulgaria*. Map M 1:600 000. Sofia: Prof. M. Drinov Acad. Publ..
- [18] D. Peev, (2011), *Red Data Book of Republic of Bulgaria*. vol. 1. Plants and Fungi. Sofia: IBER – BAS & MEW.
- [19] K. Haydu, (2012), *Mapping Plant Biodiversity Hotspots at the County Scale: A New Tool for Establishing Resource Conservation Strategies*, Ph.D. thesis, San Luis Obispo: Cal Poly State University.
- [20] N. Myers, (1990), The biodiversity challenge: expanded hot-spots analysis," *The Environmentalist*, vol. 10, no. 4, pp. 243-256, 1990. <https://doi.org/10.1007/BF02239720>.
- [21] D. Khakurel, Y. Uprety, S. Karki, B. Khadka, B. D. Poudel, G. Ahn, J.-Y. Cha, W.-Y. Kim, S.-H. Lee, S. Rajbhandary, (2024), Assessing the risks to valuable medicinal plants in Nepal from human activities and environmental factors, *Global Ecology and*

Conservation, vol. 51, e02860, 2024.

<https://doi.org/10.1016/j.gecco.2024.e02860>.

- [22] R. Kumar, D. Arya, K. C. Sekar, M. Bisht, (2021), Threat Assessment and Prioritization of High-Value Medicinal Plants in

Pindari Valley, Nanda Devi Biosphere Reserve, India, Curr World Environ, vol. 16, no. 1, <http://dx.doi.org/10.12944/CWE.16.1.24>

- [23] N. Myers, R. Mittermeier, C. Mittermeier, G. da Fonseca and J. Kent, (2000), Biodiversity hotspots for conservation priorities, Nature, 403, 853-858, 2000. <https://doi.org/10.1038/35002501>

Critical Infrastructure Risk Assessment Approach

Zarko I. Zdravkov

Rakovski National Defence College
Defence Advanced Research Institute
Sofia, Bulgaria
z.zdravkov@rndc.bg

Ivo G. Radulov

Rakovski National Defence College
Defence Advanced Research Institute
Sofia, Bulgaria
i.radulov@rndc.bg

Abstract—The paper focuses on the activities for improving protection of critical infrastructures and in particular a methodology for the risk assessment of CI assets of the Ministry of Defence (MoD) of the Republic of Bulgaria is presented. It defines the stages through which this process takes place and proposes a mathematical apparatus including analytical expressions for risk assessment. The methodology reveals how experts can measure, document and report risk in this area. It uses universal mathematical models for risk assessment based on adapted scientific theories and methods making it applicable to risk assessment for other CI assets in Bulgaria.

Keywords—critical infrastructure, risk, risk management

I. INTRODUCTION

Effective risk management requires the application of a systematic approach related to the identification, assessment and mitigation of potential threats to critical infrastructure assets in Bulgaria. This includes the development of strategies to prevent the occurrence of risk events, prepare for crisis response, and identify activities to restore damage after these events occur. Establishing a unified risk management methodology will allow organizations whose responsibilities are related to this topic to implement best practices and procedures for protecting critical infrastructure assets.

The proposed methodology into this article has been developed for the purposes of the Ministry of Defence (MoD) of the Republic of Bulgaria. It has been successfully approved since 2017. It is original, with a low degree of complexity, which is a prerequisite for its successful application in practice. Into the methodology have been applied universal mathematical models for risk assessment based on adapted scientific theories and methods which makes it applicable to all CI assets in the Republic of Bulgaria.

II. MATERIALS AND METHODS

By definition, risk is a function of the probability of a risk event occurring and its consequences. To make the result more accurate, another component is added to this

function in this methodology - the influence of the vulnerabilities of the CI assets. Thus, the risk score becomes the product of the probability (P) of a risk event occurring, the influence of the vulnerabilities (V) of the CI assets and the impact (I) of the risk event occurring for each individual asset.

$$R = P \cdot V \cdot I \quad (1)$$

The assessment of the probability of a risk event occurring is done in linguistic qualitative terms with the help of experts. The coding of probabilities with numerical values is given in Table 2.

The other necessary component for risk assessment in the identified CI-s and their assets is their vulnerability to occurrence of the identified risk event. The assessment of the vulnerabilities for a given CI site is performed by experts with experience in the relevant field. For their convenience, a questionnaire can be prepared to list the vulnerabilities. For each vulnerability, countermeasures shall be listed, if any. Where countermeasures are available for existing vulnerabilities, the experts assess their aggregate effectiveness in the range of 0 to 100%.

The next main component of the risk assessment is the consequences of a risk event. This is done by assessing losses through qualitative measures that are translated into quantitative (monetary) ones. Losses are classified according to a material loss classification scale (see Table 4).

Risk is a function of the elements listed above and is calculated as the product of the three values. The result is a rank number derived from the conditionally separated intervals for the five risk levels for each individual risk event (see Table 5).

Figure 1, Stage 2 illustrates the general sequence of steps required by the risk management process. (ISO 31000:2018 - Risk management)

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.23>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

III. RESULTS AND DISCUSSION

A. Assumptions and constraints

In mathematical modelling it is almost always necessary to make simplifying propositions. The presented Methodology has been carried out under assumptions and constraints imposed by the specificity of the subject matter and by the lack of sufficient information on certain controllable and/or independent variables and parameters as well as on the interactions between them.

In order to achieve the objective of the Methodology, the following assumptions have been made:

- Critical infrastructures and their assets are identified a priori by experts in accordance with the established procedure in the Ordinance on the Procedure, Method and Competent Authorities for the Identification of CIs and their assets and Risk Assessment, in force since 23 Oct. 2012, adopted by Council of Ministers Decree No. 256 of 17 Oct. 2012 [2] [3];
- the possible risk events for a critical infrastructure asset are:

1. disasters - fire (forest, field); flood; earthquake; landslide and collapse; snow and ice; fire caused by an accident at the site; explosion and/or nuclear, chemical and bacteriological event caused by an accident at and/or outside the site by the CI;

2. acts of terrorism, as well as individual acts of organized crime that directly threaten the security of citizens and critical infrastructure [4].

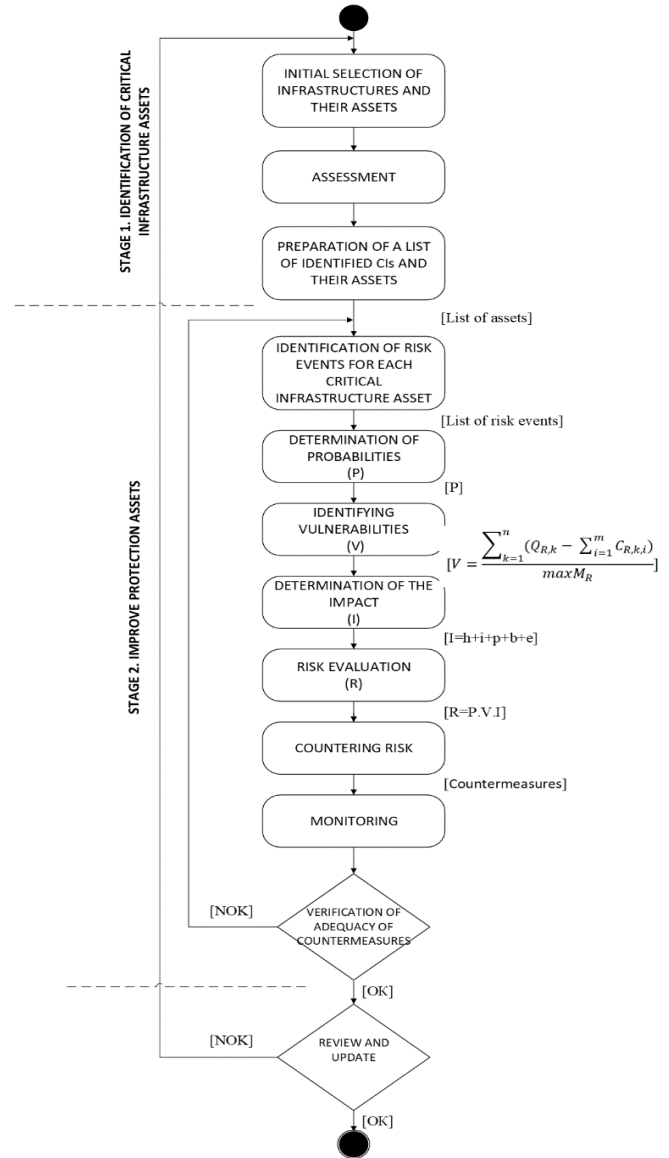


Fig. 1. Model for risk management of Critical Infrastructure.

Constraints:

- Connectivity of assets in a common infrastructure is not taken into account. Indirect damages caused by direct or indirect action of the CI site are not valued;
- A risk assessment model without risk accumulation is used. Risks are assessed individually and not in combination, i.e. it is not considered that a single risk may lead to the occurrence of a second risk, which in turn leads to the occurrence of a third risk, and so on, until set objectives fail;
- The following risks are not considered: 1) disasters caused by drought, violent winds, tornadoes, dust storms, hailstorms, sea storms, outbreaks of contagious diseases and epidemics in humans, animals and plants; 2) space, aviation, rail, road, vessel and unintentional accidents [4].

B. Risk events identification

Optimally, risk identification should take into account all possible hazards, their probability of occurrence and their likely impact, but such a complex approach is difficult to achieve in practice.

In order to simplify the process of identifying risk events, this Methodology presents scenario development questions relating to the occurrence of the identified risk events. This limits the number of situations and determines which risk to analyze in the next steps. This is a cyclical process and if additional risks are subsequently identified, they must be taken into account for further analysis [5].

Using clarifying questions, Table 1 presents several scenarios to identify possible risk events. The questions are answered with YES or NO, thus forming the list of risk events. Only those events are taken into account for which the answer to the question about the scenario coming true is affirmative.

TABLE I. QUESTIONS TO IDENTIFY RISK EVENTS

№	 (Name of critical infrastructure facility)	
	Scenarios for the occurrence of potential risk events (Clarifying question to identify them)	Response
Disasters		
1.	Fire (forest, field): Is it possible that a CI fire at the site could be caused by the ignition of a field, belt or woodland in the vicinity?	YES/NO
2.	Flood: Is flooding of the CI site possible due to being in the catchment area of a river or other water body?	YES/NO
3.	Earthquake: Are there possible consequences/damages to the CI site due to being located in a seismic hazard area?	YES/NO
4.	Landslide: Are there possible consequences/damages to the CI site the due to being in a landslide area?	YES/NO
5.	Snow and Ice: Is it possible to disrupt the CI site's performance due to its location within areas covered in snow and ice?	YES/NO
6.	Nuclear, chemical and bacteriological event due to off-site accident: Are there possible impacts to the CI site due to being in the contamination source area?	YES/NO
7.	Fire arising from an accident: Is a fire likely to occur at the CI site as a result of the presence of flammable and combustible substances and materials?	YES/NO
8.	Explosion caused by accident: Are there possible consequences/damage to the CI site as a result of an accident with explosive materials present?	YES/NO
9.	Nuclear, Chemical and Bacteriological Event arising from an accident at the Site: Are there possible consequences/damages to the CI site arising from the handling of nuclear, chemical and bacteriological materials?	YES/NO
Terrorist acts		
10.	Internal: Are there internal contradictions that could lead to a terrorist attack?	YES/NO
11.	External: Are there external socio-political contradictions that could lead to a terrorist attack?	YES/NO

C. Probabilities determination

Determining the probability (P) of a risk event occurring is done in linguistic qualitative terms through expert judgment. An exponential distribution was used to determine the probability scale. The estimation of probabilities is coded using Table 2.

TABLE II. PROBABILITY CODING

Ratio	Description of probability (Expert scale)	Interval
0,2	Practically impossible	$[0 \div 10^{-4}]$
0,5	Unlikely	$(10^{-4} \div 10^{-2}]$
1,0	Possible in certain cases	$(10^{-2} \div 0,10]$
3,0	Below average	$(0,10 \div 0,20]$
5,0	Medium	$(0,20 \div 0,35]$
7,0	Above average	$(0,35 \div 0,55]$
10,0	High	$(0,55 \div 1,00]$

D. Identifying vulnerabilities

TABLE III. DETERMINATION OF VULNERABILITIES AND PERFORMANCE MEASURES

The prerequisite for the occurrence of the R^{th} risk event M_R is calculated using the formula:

In this stage, the vulnerabilities associated with the

..... (Risk event name)								
	Vulnerability		Countermeasure effectiveness C _R (%)				$\sum_{i=1}^m C_{R,k,i}$	$Q_{R,k} - \sum_{i=1}^m C_{R,k,i}$
	Question	Value						
1.	Q _{R,1}	0 or 1	C _{R,1,1}					
2.	Q _{R,2}	0 or 1	C _{R,2,1}	C _{R,2,2}	C _{R,2,3}			
3.	Q _{R,3}	0 or 1						
								
k.	Q _{R,k}	0 or 1						
Number of vulnerabilities		maxM _R						$M_R = \sum_{k=1}^n (Q_{R,k} - \sum_{i=1}^m C_{R,k,i})$
Prerequisite for the risk event								

identified risk event for the specific asset are recorded. A "cross-section" of vulnerabilities with potential threats is made. Given a lack of relationship between a potential hazard and existing asset vulnerability, no risk is assessed, i.e. it is not possible for such a hazard to affect the performance of the asset. A questionnaire is developed for each of the recorded potential risk sources. Answering a specific question determines the potential vulnerabilities of the identified risk events for each specific CI site.

The following analytical expression is used to calculate the impact of existing vulnerabilities (VR) and their countermeasures against the probability of the risk event occurring:

$$V_R = \left(\frac{M_R}{maxM_R} \right) \quad (2)$$

where: index R denotes the specific risk event;

M_R - prerequisite for the occurrence of the R^{th} risk event;

$maxM_R$ - maximum value of vulnerabilities defined by questions for occurrence of the R^{th} risk event.

For each risk event, M_R and $maxM_R$ are calculated. The premise for the occurrence of R (M_R) is defined as the difference between the value of each vulnerability and the effectiveness of the measures applied to mitigate it.

Vulnerability is calculated by answering each question regarding a risk event with either YES or NO. The purpose of each question is to determine the presence of vulnerability. For the purposes of the Methodology, the following is assumed:

- If YES, the question is assigned a value of 1 (vulnerability exists);
- If NO, the question is assigned a value of 0 (no vulnerability).

$$M_R = \sum_{k=1}^n (Q_{R,k} - \sum_{i=1}^m C_{R,k,i}) \quad (3)$$

where: n - number of questions directed at the R^{th} risk event;

m - number of countermeasures against a vulnerability defined by n^{th} question;

$Q_{R,k}$ - question that detects a vulnerability (takes the value 1 or 0 depending on the answer for the k^{th} question);

$C_{R,k,i}$ - effectiveness of the i^{th} countermeasure against the vulnerability from the k^{th} question (evaluated in percentage);

$\sum_{i=1}^m C_{R,k,i}$ - aggregated effectiveness of complementary i number of measures for this vulnerability (assumes a value from 0 to 100%).

Effectiveness values for complementary measures (where there is more than one measure for the same risk event) are distributed up to 100%. The resulting parameters are transferred in Table 3.

Note: Aggregated efficiency ($\sum_{i=1}^m C_{R,k,i}$) of complementary i number of measures for each vulnerability assumes a value from 0 to 100%.

$maxM_R$ is a function of vulnerability detection issues:

$$maxM_R = n, \quad (4)$$

where: n – number of YES questions

E. Determination of the impact

The negative consequences of the occurrence of risk events are calculated on the basis of a valuation of the losses when critical assets of the objects are affected, namely [6]:

- human losses (h);

- information (i);
- processes (functions) (p);
- buildings and structures (b);
- machinery and equipment (e).

The valuation of losses is entered for each asset affected as the total is calculated through the following formula:

$$I = h + i + p + b + e \quad (5)$$

The human losses (h) are calculated by the formula:

$$h = t(\sum_{k1=1}^n (h1_{k1} + h2_{k1}) + \sum_{k2=1}^m h3_{k2}) \quad (6)$$

where: n - number of dead;

m - number of injured;

t - coefficient of loss of public confidence;

$h1_{kl}$ - financial means of compensation for the death of the k^{l-st} victim;

$h2_{kl}$ - financial resources for the selection and training of an officer to replace the k^{l-st} victim (to be entered only when the deceased is an employee of the establishment concerned);

$h3_{k2}$ - financial resources for treatment and recovery.

The loss of public confidence in human casualties is captured by the loss of public confidence factor (t). Using the following semi-quantitative scales, it can take the following values: (1) limited/not significant, (2) minor/significant, (3) moderate/serious, (4) significant/very serious, and (5) catastrophic/disastrous. Most common value of “ t ” is 2.

The information loss (i) is calculated by the formula:

$$i = \sum_{k1=1}^n i1_{k1} + t \sum_{k2=1}^m i2_{k2} \quad (7)$$

where: n - number of destroyed information units¹;

m - number of information units with breached confidentiality;

t - coefficient of loss of public trust;

$i1_{kl}$ - financial means for the recovery of the kl^{st} information unit;

$i2_{k2}$ - financial means to recover the $k2^{nd}$ information with breached confidentiality.

Similarly, to the previous case, the decrease in public trust upon loss of confidentiality is accounted for by multiplying the resulting value by a factor of 2.

The process loss (p) is calculated using the formula:

$$p = \sum_{k=1}^n p_k \quad (8)$$

where: n - number of disrupted processes;

p_k - lost financial resources from lost benefits of the k^{th} function.

Losses (damages) to buildings and structures (b) are calculated using the formula:

$$b = \sum_{k=1}^n (b1 + b2)_k \quad (9)$$

where: n - number of buildings and structures affected;

$b1_k$ - financial resources lost from damage to the building or facility;

$b2_k$ - financial resources for reconstruction of the k^{th} building or facility.

The loss of machinery and equipment (e) is calculated by the formula:

$$e = \sum_{k=1}^n e_k \quad (10)$$

where: n - number of destroyed and/or damaged machinery and equipment;

e_k - financial resources for the purchase, delivery and installation of the machinery and/or equipment or financial resources for repairs.

After finding the losses (I) as the sum of the additives in formula (5), a classification of the amount of material losses is made based on their position on the limiting interval of the scale in Table 4. The relevant coefficient from Table 4 is substituted into the risk calculation formula. The result is a dimensionless rank number.

TABLE IV. CLASSIFICATION OF MATERIAL LOSSES

Ratio	Description of the losses	Amount of losses (Million Euro)
1,0	Small	[0 - 3,5]
3,0	Significant	(3,5 - 12]
7,0	Serious	(12 - 48]
15,0	Hazardous	(48 - 100]
40,0	Catastrophic	above 100

F. Risk evaluation

A risk evaluation is made for each CI asset using formula (1).

Risk evaluation is a specific type of activity in which the results of the analysis are compared with the risk criteria to determine whether the risk is acceptable or unacceptable. Risk evaluation is also concerned with the grading of risks to determine their importance and priority. The grading and prioritization of risks is carried out in accordance with the

¹ Valuable information

scale adopted in Table 5, thus concluding which of the identified risks should be managed [7].

TABLE V. CODING OF RISK LEVELS

Grade	Rank	Description
I	(0 - 2]	Negligible, too limited- no attention needed
II	(2 - 5)	Acceptable - attention needed
III	[5 - 35]	Moderate - measures needed to reduce it
IV	[35 - 200]	Serious - measures should be taken immediately
V	> 200	High - cessation of activity until the risk is eliminated

The rank number obtained from formula (1) is coded into five levels of importance. For the first two levels of risk (negligible and acceptable) no special measures are needed. The III level, signifying a moderate risk, is marked in yellow, meaning measures are needed to reduce it. The last two levels of risk (serious and high) are visualized in red and demand special attention to be addressed.

When substituted with the possible probability, vulnerability and consequence values, the risk matrix appears in the format shown in Figures 2 to 6.

V/P	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,02	0,04	0,06	0,08	0,10	0,12	0,14	0,16	0,18	0,20
0,5	0,05	0,10	0,15	0,20	0,25	0,30	0,35	0,40	0,45	0,50
1	0,10	0,20	0,30	0,40	0,50	0,60	0,70	0,80	0,90	1,00
3	0,30	0,60	0,90	1,20	1,50	1,80	2,10	2,40	2,70	3,00
5	0,50	1,00	1,50	2,00	2,50	3,00	3,50	4,00	4,50	5,00
7	0,70	1,40	2,10	2,80	3,50	4,20	4,90	5,60	6,30	7,00
10	1,00	2,00	3,00	4,00	5,00	6,00	7,00	8,00	9,00	10,00

Fig. 2. Risk rank numbers calculated for impacts = 1 (small), probabilities (P) from 0.2 to 10 (by row), and vulnerabilities (V) from 10 to 100% (by column)

V/P	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,06	0,12	0,18	0,24	0,30	0,36	0,42	0,48	0,54	0,60
0,5	0,15	0,30	0,45	0,60	0,75	0,90	1,05	1,20	1,35	1,50
1	0,30	0,60	0,90	1,20	1,50	1,80	2,10	2,40	2,70	3,00
3	0,90	1,80	2,70	3,60	4,50	5,40	6,30	7,20	8,10	9,00
5	1,50	3,00	4,50	6,00	7,50	9,00	10,5	12,0	13,5	15,00
7	2,10	4,20	6,30	8,40	10,5	12,6	14,7	16,8	18,9	21,00
10	3,00	6,00	9,00	12,0	15,0	18,0	21,0	24,0	27,0	30,00

Fig. 3. Risk rank numbers calculated for impacts = 3 (significant), probabilities (P) from 0.2 to 10 (by row) and vulnerabilities (V) from 10 to 100% (by column)

V/P	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,14	0,28	0,42	0,56	0,70	0,84	0,98	1,12	1,26	1,40

V/P	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,5	0,35	0,70	1,05	1,40	1,75	2,10	2,45	2,80	3,15	3,50
1	0,70	1,40	2,10	2,80	3,50	4,20	4,90	5,60	6,30	7,00
3	2,10	4,20	6,30	8,40	10,5	12,6	14,7	16,8	18,9	21,00
5	3,50	7,00	10,5	14,0	17,5	21,0	24,5	28,0	31,5	35,00
7	4,90	9,80	14,7	19,6	24,5	29,4	34,3	39,2	44,1	49,00
10	7,00	14,0	21,0	28,0	35,0	42,0	49,0	56,0	63,0	70,00

Fig. 4. Risk rank numbers calculated for impacts = 7 (severe), probabilities from 0.2 to 10 (by row) and vulnerabilities from 10 to 100% (by column)

V/P	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,30	0,60	0,90	1,20	1,50	1,80	2,10	2,40	2,70	3,00
0,5	0,75	1,50	2,25	3,00	3,75	4,50	5,25	6,00	6,75	7,50
1	1,50	3,00	4,50	6,00	7,50	9,00	10,5	12,0	13,5	15,00
3	4,50	9,00	13,5	18,0	22,5	27,0	31,5	36,0	40,5	45,00
5	7,50	15,0	22,5	30,0	37,5	45,0	52,5	60,0	67,5	75,00
7	10,5	21,0	31,5	42,0	52,5	63,0	73,5	84,0	94,5	105,0
10	15,0	30,0	45,0	60,0	75,0	90,0	105	120	135	150,0

Fig. 5. Risk rank numbers calculated for impacts = 15 (hazardous), probabilities (P) from 0.2 to 10 (by row) and vulnerabilities (V) from 10 to 100% (by column)

V/P	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,80	1,60	2,40	3,20	4,00	4,80	5,60	6,40	7,20	8,00
0,5	2,00	4,00	6,00	8,00	10,0	12,0	14,0	16,0	18,0	20,0
1	4,00	8,00	12,0	16,0	20,0	24,0	28,0	32,0	36,0	40,0
3	12,0	24,0	36,0	48,0	60,0	72,0	84,0	96,0	108	120,0
5	20,0	40,0	60,0	80,0	100	120	140	160	180	200,0
7	28,0	56,0	84,0	112	140	168	196	224	252	280,0
10	40,0	80,0	120	160	200	240	280	320	360	400,0

Fig. 6. Risk rank numbers calculated for impacts $I = 40$ (catastrophic), probabilities (P) 0.2 to 10 (by row) and vulnerabilities (V) 10 to 100% (by column)

The matrix is used as a means of visualizing risks in order to classify them. Each risk event is classified for itself. The values obtained from the risk evaluations for each of the identified risk events are not to be added up together and then compared according to the classification indicated. Averaging their values is also prohibited.

Prioritization of risks is necessary due to the limited resources available for the implementation of the activities for the protection of assets from CI and for the management of the associated risks. For this reason, it is not possible to take effective measures to reduce the impact of all identified risks. The significance of the different risks changes during the course of the activities under the influence of internal and external factors. Therefore, it is important to know the significant risks at any time to develop countermeasures against them [7, 8]. There are four cases in which the assessed risks may not be mitigated:

- with a negligible probability of the risks occurring;
- where the impact of the risks is unrelated to the implementation of the activity;
- where the magnitude of the expected impacts is insignificant for the CI site;
- where the sources of risk are beyond the scope and extent of the specific activity.

G. Mitigating risk

Mitigating risks to CI assets is the process of selecting and implementing measures to reduce a particular risk to specified acceptable levels. This process defines the exact content of the countermeasures, the time necessary to implement them, the persons involved in the processes and their functions [9].

Countermeasures can be aimed at reducing the probability of a risk occurring, reducing vulnerabilities, limiting the magnitude of expected consequences or at all three simultaneously.

The development of risk countermeasures may require collaboration and cooperation with various internal and external to the organization entities.

A key requirement for risk countermeasures is that they are cost-effective, efficient and efficacious. Measures are specific to each CI site and each risk event associated with it. They must be appropriate to the risk countermeasure strategy adopted by the organization.

H. Monitoring

To achieve the desired effectiveness of the risk management process, ongoing and periodic monitoring and reporting of identified risks and actions taken to minimize (mitigate) them are required. CI site managers should review the entire risk register once a year. Particular risks may also be reviewed more frequently (monthly) due to their specificity and level of importance. The risk register may be updated on an ad hoc basis if changes in the environment occur.

The risk analysis and assessment information are formed as a risk management report.

IV. CONCLUSION

This paper is the second in a series that describes the Model for risk management of Critical Infrastructure (CI) of the Republic of Bulgaria. The first one [1] focuses on

activities of developing rules and proposing a mathematical apparatus for identifying critical infrastructures and their assets.

Into this paper is proposed Methodology sets out the general approach to risk management for identified critical infrastructures and their assets. The stages through which this process takes place are defined. A mathematical apparatus that includes analytical expressions for risk assessment is proposed. In this way, the theoretical foundations of risk management are linked to the practical application aspects of the Methodology.

The Methodology reveals how experts can measure, document and report risk in this area.

The success of risk management for critical infrastructures and their assets depends heavily on the adaptation of the proposed methods in practice.

The Methodology overcomes the lack of a risk management toolkit for critical infrastructures and their assets. It incorporates the best existing practices in the field, making it applicable to users beyond the scope of the intended target group. This is what determines its relevance, and its usefulness will hopefully be appreciated by all those interested in this subject.

Based on the proposed methodology, a software application MORis® has been developed to automate the risk assessment and management process for the identified critical infrastructures and their sites in the defence sector.

ACKNOWLEDGMENT

The document was developed under the National Scientific Programme "Security and Defence", funded by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

REFERENCES

- [1] Radulov I., Dimitrov T., Zdravkov Z., Petrov Zh., "Model for risk management of Critical Infrastructure of the Republic of Bulgaria", DIGILIENCE 2024-ISIJ 55: Open Source Intelligence, Artificial Intelligence, and Human-centered Approaches to Cybersecurity and Countering Disinformation (2024): 44-54, ISSN 0861-5160, e-ISSN 1314-2119, Available: https://www.researchgate.net/publication/385578897_Model_for_Risk_Management_of_Critical_Infrastructures_of_the_Republic_of_Bulgaria [last viewed: 27 May 2026].
- [2] Ordinance on the Procedure, Method and Competent Authorities for the Identification of CIs and their assets and Risk Assessment, in force since 23 Oct. 2012, adopted by Council of Ministers Decree No. 256 of 17 Oct. 2012.
- [3] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114> [last viewed: 04 September 2024].
- [4] Shalamanov, V., et al. "Study for the analysis and evaluation of the system for population protection and emergency response.

- White Paper on Civil Protection of the Republic of Bulgaria", Research Project No. 12 under the 2004 working program of the Standing Committee on Protection of the Population from Disasters, Accidents and Catastrophes, Available: <https://www.scribd.com/document/22546642/Analysis-and-assessment-of-the-civil-protection-system-BG-2004> [last viewed: 27 May 2026].
- [5] Risk Assessment and Mapping Guidelines for Disaster Management. SEC(2010)1626 final, EUROPEAN COMMISSION, Brussels, 21.12.2010.
- Tagarev T., Pavlov N., "Planning Measures and Capabilities for Protection of Critical Infrastructures", Information & Security: An International Journal, 22, (2007): 38-48. Available: https://www.researchgate.net/publication/269834426_Planning_Measures_and_Capabilities_for_Protection_of_Critical_Infrastructures [last viewed: 27 May 2026].
- [6] A Complete Guide to Risk Prioritization Matrix. Best Practices, Tools, and More, July 23rd, 2024, Available: <https://www.6sigma.us/six-sigma-in-focus/risk-prioritization-matrix/> [last viewed: 17 September 2024].
- [7] Stoyanov, V., Zlateva, P., Kirov, G., Stoyanov, K. "Application of fuzzy logic in forecasting potential losses from natural disasters". Second National Scientific and Practical Conference on Emergency Management and Population Protection, BAS, Sofia, 2007.
- [8] Georgiev, V., Risk Management as a Tool of Program Management. Sofia, Military Journal, 2005.

Improving Disaster, Accident, Emergency and Crisis Management Systems in Bulgaria

Viara Zhekova

Security and Defence Management Department
(National Security and Defence Faculty)

G. S. Racovski National Defence College

Sofia, Bulgaria

v.jekova@rndc.bg

ORCID: [0009-0007-7037-3653](https://orcid.org/0009-0007-7037-3653)

Abstract - The modern New World – the World of the 21st century – has turned out to be a world existing in a series of crises and conflicts of the most diverse nature and scope, both at the local, regional and global levels. Crisis situations are sometimes caused by man, but sometimes they are of a natural or mixed nature. In this context, serious issues facing every government and community – be they local, national, regional or supra-national – are issues related to the anticipation, timely identification and rapid adequate response to such crisis situations.

In this sense, the issue of the state of disaster, accident, emergency and crisis management systems, as well as the possibilities for their improvement, is of particular importance not only for Bulgaria as a sovereign state, but also for all countries, in a regional, allied and global aspect. In this line of thought, it is a good idea to ask the question and analyse the relationship and interaction between disaster, accident, emergency and crisis management systems with a country's national security system.

Keywords— Globalization, management, crises, security.

I. INTRODUCTION

The modern New World – the World of the 21st century, has turned out to be a world existing in a series of crises and conflicts of the most diverse nature and scope, both at the local, regional and global levels. Crisis situations are sometimes caused by man, but they also happen to be of a natural or mixed nature. In this context, serious issues facing every government and community – be they local, state, regional or supra-national – are issues related to the anticipation, timely identification and rapid adequate response to crisis situations, overcoming, prevention [1], monitoring and risk management with regards to them.

In this sense, of particular importance not only for Bulgaria as a sovereign state, but also in a regional, allied, and global aspect for all countries, the question of the state of disaster, accident, emergency and crisis management systems, as well as the possibilities for their improvement, comes to the fore. In this line of thought, it is a good idea to ask the question and analyse the relationship and interplay between disaster, accident, emergency and crisis management systems with the country's national security system. In the end, this is how the fundamental rights of the Bulgarian citizens, laid down in the Constitution of the Republic of Bulgaria [2], are guaranteed. This is how the purpose of the present development is outlined: analysis of the connection and interaction of disaster, accident, emergency and crisis management systems with the country's national security system.

Actuality of the subject is determined by the fact that security is the basis of the prosperity of any nation. Citizens want to feel safe and free from danger and/or threat. Today, however, the security of the state and its citizens confronts the rulers with challenges in all aspects of our daily lives, and the role of the institutions that are supposed to protect us is also changing. The issue of public-private partnership in this area is becoming more and more relevant.

Without a doubt, this is one of the current issues of our time, difficult, provocative, demanding, and imposing: to discipline, adaptation, foresight, and preparedness, of everyone and everything; most of all, however, in our opinion, of the national state in the context of the social contract - for protection, for care, for responsibility, which is assumed by this contract to its citizens. And here come the questions of honesty, morality, ethics, preparedness, valour, knowledge, cognition, contacts, speed, conscience... A difficult, weighty topic, especially nowadays. In this sense, in this paper, given the volume set by the organizers of this forum, we will limit ourselves, and with that we will also limit the set goal to a brief

Online ISSN 3044-7771

<https://doi.org/10.68302/std2026.vol1.214>

© 2026 The Author(s). Published by Green Future Technologies.

This is an open-access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

overview of the institutional readiness of the Republic of Bulgaria in terms of the availability in the country of disaster, accident, emergency and crisis management systems and the options for their improvement.

The methods used to achieve the goal of the present development are theoretical analysis and synthesis, comparative analyzes and a systematic approach.

Results, that we would like to achieve with this development, are: establishing the current state of the institutional readiness of the Republic of Bulgaria regarding the availability in the country of disaster, accident, emergency and crisis management systems, and the availability of opportunities for their improvement.

II. CRISIS MANAGEMENT SYSTEMS IN BULGARIA

At the beginning of the new century, humanity is shaken by serious problems of global scope, caused by both nature, and man. The realities in which we are immersed - pandemics, regional wars, terrorist acts, ambitions for dominance and influence in the form of nationalism and chauvinism, fundamentalist ideologies and religious fanaticism, economic crises, catastrophes, industrial accidents, street violence, etc., are often accompanied by serious consequences. These lead to emergency situations of varying degrees of intensity, which can have significant negative consequences on society and the overall infrastructure (and not only) of a given country, or region. In our opinion, management should categorically be and is an integral part of the national security of each country and an essential element of its protection activities. The strategic goal of crisis management policy is to prevent their occurrence, to limit the negative consequences, as much as possible, and to quickly restore the functioning of state and public life in the event of a crisis.

When raising the issue of disaster, accident, emergency and crisis management systems in Bulgaria, and even more so, their improvement, it is appropriate to start with the fact that the country today has a well-established regulatory framework regulating the above-mentioned issues and phenomena. It is based largely on the Disaster Protection Act, Promulgated by the Official Gazette No. 102 of December 19, 2006, amended by the Official Gazette No. 41 of May 22, 2007, ..., amended and supplemented by the Official Gazette No. 60 of July 7, 2020 [3], and the Management and Functioning of the National Security Protection System Act, Promulgated by the Official Gazette No. 61 of August 11, 2015, amended by the Official Gazette No. 94 of November 13, 2018, amended by the Official Gazette No. 69 of August 4, 2020, supplemented by the Official Gazette No. 61 of August 11, 2015. SG. No. 15 of February 22, 2022, amended SG. No. 90 of October 28, 2025, amended and supplemented OG. No. 94 of November 4, 2025 [4], to the Defence and Armed Forces Act of the Republic of Bulgaria, published

OG. No. 35 of May 12, 2009, amended OG. No. 74 of September 15, 2009, ..., amended and supplemented OG. No. 100 of November 25, 2025, amended OG. No. 101 of November 27, 2025, amended OG. No. 16 of February 10, 2026 [5], to the Counteracting Terrorism Act, published by OG. No. 103 of December 27, 2016, supplemented by OG No. 51 of June 5, 2020, amended by OG No. 69 of August 4, 2020, amended by OG No. 20 of March 9, 2021, amended by OG No. 15 of February 22, 2022, amended by OG No. 32 of April 26, 2022, amended by OG No. 61 of July 29, 2025 [6].

Until 2009, the Crisis Management Act (repealed, OG, issue 35 of 2009) [7] was in force in the Republic of Bulgaria. It regulates the powers of government bodies and local self-government bodies, the rights and obligations of individuals and legal entities in crisis management. It stipulates that it shall not be applied when declaring a "state of war", "martial law" or "state of emergency" within the meaning of the Defence and Armed Forces Act of the Republic of Bulgaria. Until the adoption of the Crisis Management Act in 2005, a crisis response system was established and functioning in the country, mainly related to the protection of the population during disasters, accidents and catastrophes. This is regulated by the Regulations on the organization and activities for the prevention and liquidation of the consequences of disasters, accidents and catastrophes [8], adopted by Decree No. 18 of the Council of Ministers of 1998. The organization established by the Regulations, along with its positive aspects, poses certain difficulties for crisis management. However, the Regulations do not define the procedure for the Council of Ministers, as the central body of the executive power, in cases where crises cover a larger part of the country's territory, or significantly threaten the interests of society, or the state. Last but not least, the organization established by the Regulations does not fully correspond to the crisis management systems established in the member states of the North Atlantic Treaty Organization (NATO) and the European Union, as well as by other international organizations and countries. The analysis of the regulatory framework in the field of crises before the adoption of a special Act in 2005 shows that dozens of laws and numerous other regulatory acts were in force in the country for the management of various types of crises. Last, but not least, the number of international treaties that the Republic of Bulgaria has ratified as a party, should also be taken into account. In this context, after 2001, the country became aware of the need to create a national crisis response system, through which the functions of the state to guarantee the life and wellbeing of the population and protect the spiritual and material values of the country and its citizens in the event of a crisis, were ensured.

In response to the changes that have occurred, globally and regionally, the membership of the Republic of Bulgaria in NATO and its upcoming accession to the European Union, specific legislative actions were taken, as a result of which, on February 17, 2005, the 39th National

Assembly adopted the Crisis Management Act [7]. The adopted act largely regulates public relations with regard to the prevention, control and overcoming of the consequences of crises.

Based on the comprehensive modern regulatory framework currently in force in the Republic of Bulgaria, a number of strategic documents have been adopted by the country that regulate relations between institutions. Among the strategic documents currently in force in the Republic of Bulgaria, we can mention: the National Disaster Risk Reduction Program 2021-2025, published by the Council of Ministers, Sofia 2020 [9]; the National Disaster Risk Profile of Bulgaria [10]; the Disaster Risk Management Plan [11]; Decision of the Council of Ministers No. 740/28.10.2021 on the adoption of a of Voluntary Formations Development Strategy for the Prevention or Management of Disasters, Wildfires and Other Emergency Situations in the Period 2021 – 2030 [12]; for the Development of Voluntary Formations Strategy for the Prevention or Management of Disasters, Wildfires and Other Emergency Situations in the Period 2021 - 2030; Decision of the Council of Ministers No. 758/12.10.2022 on the adoption of the National Program for the Development of Voluntary Formations for the Prevention or Management of Disasters, Wildfires and Other Emergencies in the Republic of Bulgaria for the Period 2022 – 2026 [13]; National Program for the Development of Voluntary Formations for the Prevention or Management of Disasters, Wildfires and Other Emergencies in the Republic of Bulgaria for the Period 2022 - 2026; Plan for 2026 for the Implementation of the National Program for the Development of Voluntary Formations for the Prevention or Management of Disasters, Wildfires and Other Emergencies in the Republic of Bulgaria for the Period 2022 – 2026 [14]; Program for the Modernization and Technical Provision of the Territorial Units for Fire Safety and Protection of the Population in the Republic of Bulgaria [15]; Oil Spills in the Black Sea Combating National Emergency Plan [16]; Kozloduy NPP External Emergency Plan [17], etc.

In our opinion, another interesting and important document is the development of a strategy and system for Emergency Situations, Disasters and Accidents Management. It was developed under the SUDEM (Sustainable Disaster and Emergency Management processes) project with Bulgarian participation. It is important to emphasize, in the present-day context, that this is a strategy at the European level, based on digitalization. The system uses artificial intelligence and drones to increase the effectiveness of disaster and accident management actions. The strategy and the system were created under the "Sustainable Management of Disaster and Accident Activities" - SUDEM" international project, under a European Union (EU) "Erasmus +" program. There are partners in the project from the Netherlands, Germany, Ukraine and Turkey, as well as

scientists from the Institute for Space Research and Technology at the Bulgarian Academy of Sciences (ISRT - BAS). In the words of Prof. Dr. Georgi Georgiev, the coordinator of the SUDEM project: "There is a need for a system for sustainable digitalization of processes in the management of emergency situations due to the increasing frequency of climatic, anthropogenic and other emergency situations leading to disasters and accidents and the unpreparedness of countries in Europe to meet these situations". [18] Here we would like to echo the words of Prof. Dr. Dimo Zafirov from the Institute of Civil Engineering and Technology-BAS, also a party to, and active participant in the project: "We aim for dangerous phenomena not to develop into disasters. To be able to control situations with fewer casualties and material damage. In most cases, the delay in the response to dangerous phenomena and disasters is due to human reaction." [18]

It should be emphasized that numerous crises and emergencies action training centres have been established and continue to be set up in the country at the institutional and academic level. Among the good examples we can mention: The Emergency Management Training Centre at the G. S. Rakovski National Defence College, established in 2011 with the main purpose of training leaders and experts from the national and local administration, the Armed Forces and other experts in the field of disaster, accidents and environmental catastrophes management. The centre is used in the training of students, PhD students, and staffs for the implementation of disaster protection plans at national, regional and municipal levels, conducting specialized courses and computer-assisted exercises and staff training [19]. As another such example, operating in a similar vein, we can mention the Department of Disaster Medicine at the Military Medical Academy-Sofia as a key unit for training and organizing medical provision in the event of natural disasters, industrial accidents and terrorist acts. It trains military and civilian medics, develops concepts for actions in extreme situations and includes experts in military toxicology and preventive medicine [20]. There are a number of similar examples that we can give today in the country, which shows both the great interest in the topic and the awareness of its importance at every level.

Looking again at the topic thus set, namely: "Improvement of Disaster, Accident, Emergency and Crisis Management Systems in Bulgaria", it is important to note that, to date, in the Republic of Bulgaria a Disaster Risk Reduction Council has been established and operates under the supervision of Council of Ministers, to assist in the formation and implementation of government policy in the field of disaster protection in Policy Area 02. Internal order and security. The Council was established by the Disaster Protection Act to assist in the formation and implementation of government policy in the field of disaster protection. By Council of Ministers Decree No.

305 of November 17, 2016 (published in the Official Gazette, No. 93 of November 23, 2016) [21], the Procedural Rules for the Organization and Activities of the Disaster Risk Reduction Council under the Council of Ministers for Supporting the Formation and Implementation of State Policy in the Field of Disaster Protection, were adopted. The nominal composition of the Council was determined by order of the Minister of Internal Affairs and Chairman of the Disaster Risk Reduction Council. And perhaps this is the time to emphasize that, speaking of a supra-institutional body that would unite all institutions and other organizations engaged in this field, connect and coordinate them with a common policy and common actions, it is precisely the Disaster Risk Reduction Council under the Council of Ministers to assist in the formation and implementation of state policy in the field of disaster protection or another similar body that would be a good solution, with which the government, and in particular, its executive branch, as well as the citizens, would be able to have a significantly clearer vision and control over this issue, policy and field of such importance to national security.

III. CONCLUSION

Unequivocally, in our opinion, the topic of disaster, accident, emergency and crisis management systems, and their constant improvement both at the national and global levels, has been, is and remains one of the leading topics in terms of security, both at the national and global levels. The results that we can present as a result of the analysis of the present study and the necessary conclusions are that in Bulgaria, over the past 25-30 years, much has been done in this area, both in terms of the regulatory framework, and the institutional readiness of the country, as well as in terms of training at every level. There is, of course, much more to be desired and more to be done in this regard. Our country has taken numerous significant steps towards building a disaster, accident, emergency and crisis management system that meets modern requirements. There also remain a lot of challenges that our country faces in improving this system. In our opinion, the main challenge is the lack of a sufficient budget funding in an area that is extremely important for national security. And last, but not least, we will allow ourselves to make some recommendations: it is good we should look not only at good contemporary practices, but also at good practices from the past in this area, when trying to improve the system [22]. In our opinion, there is much to be learnt from past efforts, when striving to improve disaster, accident, emergency and crisis management systems in Bulgaria, as well as for the improvement and optimization of their work, which in certain circumstances could be life-saving.

The analysis of the current state of the innovation potential of disaster, accident, emergency and crisis management systems and their constant improvement shows a clear interrelationship and interdependence

between the elements of determining the scope of equipment modernization, allocating financial resources and demonstrating political will. The financial resources set aside in previous years are gradually increasing in order to acquire a better and adequate state of security for modernity and the real modern environment.

The key to successful completion of started projects is clear political will. How many former governments have already had the unpleasant experience of failed projects that lacked either adequate financial resources or political support. On the other hand, sometimes valuable financial resources are wasted on unnecessary upgrades. Balance and unity of effort are needed to achieve the intended results.

In conclusion it can be said, that the management of disaster, accident, emergency and crisis management systems depends not only on the volume of individual resources for their constant improvement, but also on how these resources are used. The increase in the efficiency of their use allows to increase the level of national security of the country, as well as the feeling of security of the citizens, and this automatically leads to an increase in the well-being of the nation.

There is much more to be said on this topic, but given the limitations set, the author will express his position on the topic in his following papers.

ACKNOWLEDGMENTS

This is publication part of the implementation of the "Security and Defence" National Scientific Program adopted by the Council of Ministers Decree No. 731 of 21.10.2021 and, according to Agreement No. D01-74/19.05.2022, is funded by the Ministry of Education and Science of the Republic of Bulgaria.

REFERENCES

- [1] Richard Lukey, *Crisis Management: Anticipating and Coping*, Publisher "Classics and Style", 2007, ISBN 9789543270286, Barcode 9789543270286
- [2] Constitution of the Republic of Bulgaria, Promulgated, SG No. 56 of 13.07.1991, in force from 13.07.1991, amended, and supplement, no. 85 of 26.09.2003, amended and supplement, No. 18 of 25.02.2005, amended, and supplement, no. 27 of 31.03.2006, No. 78 of 26.09.2006 - Decision No. 7 of the Constitutional Court of 2006, amended, and add. no. 12 of 6.02.2007, amended and add. No. 100 of 18.12.2015, amended and add. no. 106 of 22.12.2023, No. 66 of 06.08.2024 - Decision No. 13 of the Constitutional Court of 2024)
- [3] Disaster Protection Act, Promulgated by the Official Gazette No. 102 of December 19, 2006, amended by the Official Gazette No. 41 of May 22, 2007, ..., amended and supplemented by the Official Gazette No. 60 of July 7, 2020
- [4] Management and Functioning of the National Security Protection System Act, Promulgated by the Official Gazette No. 61 of August 11, 2015, amended by the Official Gazette No. 94 of November 13, 2018, amended by the Official Gazette No. 69 of August 4, 2020, supplemented by the Official Gazette No. 61 of August 11, 2015. SG. No. 15 of February 22, 2022, amended SG.

- No. 90 of October 28, 2025, amended and supplemented OG. No. 94 of November 4, 2025
- [5] The Defence and Armed Forces Act of the Republic of Bulgaria, published OG. No. 35 of May 12, 2009, amended OG. No. 74 of September 15, 2009, ..., amended and supplemented OG. No. 100 of November 25, 2025, amended OG. No. 101 of November 27, 2025, amended OG. No. 16 of February 10, 2026
- [6] The Counteracting Terrorism Act, published by OG. No. 103 of December 27, 2016, supplemented by OG No. 51 of June 5, 2020, amended by OG No. 69 of August 4, 2020, amended by OG No. 20 of March 9, 2021, amended by OG No. 15 of February 22, 2022, amended by OG No. 32 of April 26, 2022, amended by OG No. 61 of July 29, 2025 The Crisis Management Act,
- [7] Announcement, SG No. 19 of 2005, amended and supplement, no. 17, 30 and 102 of 2006, no. 11, 41 and 78 of 2007, (repealed, OG, issue 35 of 2009)
- [8] The Regulations on the organization and activities for the prevention and liquidation of the consequences of disasters, accidents and catastrophes, adopted by Decree No. 18 of the Council of Ministers of 1998
- [9] The National Disaster Risk Reduction Program 2021-2025, published by the Council of Ministers, Sofia 2020
- [10] The National Disaster Risk Profile of Bulgaria
- [11] The Disaster Risk Management Plan
- [12] Decision of the Council of Ministers No. 740/28.10.2021 on the adoption of a of Voluntary Formations Development Strategy for the Prevention or Management of Disasters, Wildfires and Other Emergency Situations in the Period 2021 – 2030
- [13] The Development of Voluntary Formations Strategy for the Prevention or Management of Disasters, Wildfires and Other Emergency Situations in the Period 2021 - 2030; Decision of the Council of Ministers No. 758/12.10.2022 on the adoption of the National Program for the Development of Voluntary Formations for the Prevention or Management of Disasters, Wildfires and Other Emergencies in the Republic of Bulgaria for the Period 2022 – 2026
- [14] National Program for the Development of Voluntary Formations for the Prevention or Management of Disasters, Wildfires and Other Emergencies in the Republic of Bulgaria for the Period 2022 - 2026; Plan for 2026 for the Implementation of the National Program for the Development of Voluntary Formations for the Prevention or Management of Disasters, Wildfires and Other Emergencies in the Republic of Bulgaria for the Period 2022 – 2026
- [15] Program for the Modernization and Technical Provision of the Territorial Units for Fire Safety and Protection of the Population in the Republic of Bulgaria
- [16] Oil Spills in the Black Sea Combating National Emergency Plan
- [17] Kozloduy NPP External Emergency Plan
- [18] BTA :: A strategy for the development of a system for managing emergencies, disasters and accidents was developed under the SUDEM project with Bulgarian participation, 2026, <https://www.bta.bg/bg/news/bulgaria/1078101-strategiya-za-razvitiie-na-sistema-za-upravlenie-na-izvanredni-situatsii-bedstvi> , 22.04.2026, 10,22 p.m.
- [19] "Emergency Management" Training Center at the "G.S. Rakovski" Military Academy, "EMERGENCY MANAGEMENT" TRAINING CENTER - "Georgi Stoikov Rakovski" Military Academy, 22/04/2026, 10:25 p.m.
- [20] Department "Medicine of disaster situations" at the Academy of Medical Sciences-Sofia, Military Medical Academy - Department, 22.04.2026, 22.30 hours
- [21] Disaster Risk Reduction Council to the Ministerial Council to Support the Formation and Implementation of State Policy in the Field of Disaster Protection, Disaster Risk Reduction Council to the Ministerial Council to Support the Formation and Implementation of State Policy in the Field of Disaster Protection, 22.04.2026, 10:35 p.m.
- [22] Collective, Successful Management in Crisis Conditions, SoftPress Publisher, 2007, ISBN 9789546855602, Barcode 9789546855602