Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 311-319

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

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.

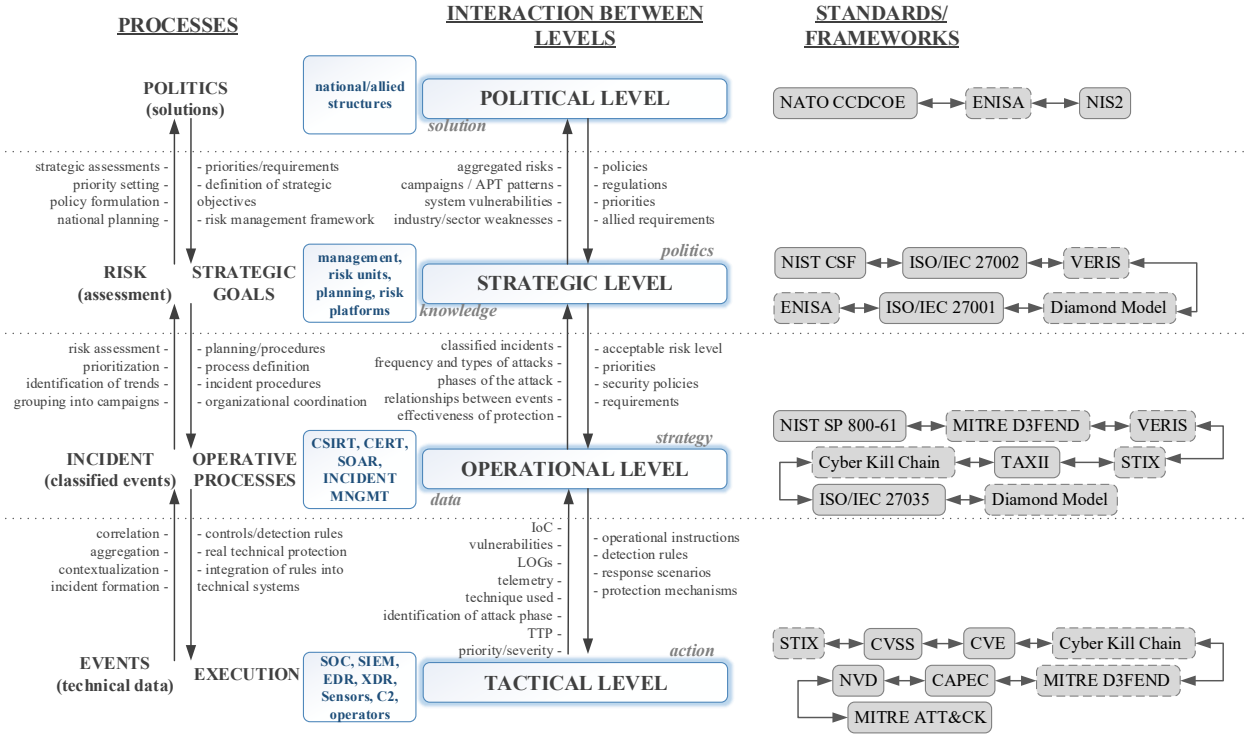

Fig. 1. Multidimensional model for managing cyber incidents in the "Security and Defense" sector.

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://ccdcoe.org/, [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.