Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 51-56

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. Ther 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

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 an 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

Ther 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' 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 inners 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.

Ther 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 / Disadvantages	Advantage: Technological sovereignty; Disadvantage: Impossibility of achieving it by the third decade of the 21st century.	Advantage: Independence from foreign interference; Disadvantage: Contradicts the needs of the information society.	Probably the most applicable policy toward cyberspace, including warfare within it. It both allows for hybrid warfare and enables cooperation in countering threats originating from cyberspace.	Advantage: None identified. 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 denotated 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 doubt;

- 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.