Elżbieta Hodyr
War Studies University
ORCID: 0000-0001-5045-093X
ehodyr@gmail.com

Military Operations in Cyberspace Before 2022: Strategic Assumptions and Doctrinal Approaches

Abstract

Cyberspace has become a key operational domain for modern armed forces, alongside land, sea, air, and space. This article examines how the United States and the Russian Federation conduct military operations in cyberspace, focusing on their official doctrines, organisational structures, and practical capabilities. The analysis highlights fundamental differences in how both countries define cyberspace and use it for offensive, defensive, and strategic purposes. Particular attention is paid to the role of electronic warfare and the integration of cyber capabilities into broader military planning. The article also considers the implications of these differences for NATO and the European Union, especially in the context of growing tensions and the evolving nature of hybrid threats.

Key words: cyberspace, military operations, electronic warfare, strategy

Introduction

To provide a clearer context for the topic under discussion, this section begins with a description of cyberspace. In 2016, during the NATO summit in Warsaw, member states decided to recognise cyberspace as the fifth domain of the battlefield, alongside land, air, sea, and space. According to the American document „Cyberspace Operations", cyberspace consists of

three interconnected layers. The physical layer includes tangible network components such as hardware and infrastructure – cables, routers, servers, and computers. The logical layer comprises the connections between network devices, including applications, data, and protocols that facilitate data exchange within the physical layer. The social layer refers to the individuals and groups engaged in cyber activities[1].

In 2011, the Office of the Prime Minister of the United Kingdom defined cyberspace in the document „The United Kingdom Cybersecurity Strategy – Protecting and Promoting the United Kingdom in a Digital World" as an interactive domain composed of digital networks used to store, modify, and transmit information. While the Internet is a part of cyberspace, it also encompasses other information systems that support business operations, infrastructure, and the delivery of services[2]. Also in 2011, the French Network and Information Security Agency (ANSSI) defined cyberspace as a communication space formed by the global interconnection of devices used for the automatic processing of digital data[3]. The authorities of the Federal Republic of Germany, in the document „Germany's Cyber Security Strategy", defined cyberspace as a virtual space comprising all information systems connected at the data level on a global scale. The foundation of cyberspace is the Internet, viewed as a universal and publicly accessible network for communication and data transport, which can be expanded by an unlimited number of additional data networks. In contrast, information systems operating in isolated virtual environments are not considered part of cyberspace[4]. NATO also defines cyberspace in the document „Cybersecurity: A Generic Reference Curriculum", where it is described as the electronic world created by interconnected information technology networks and the information contained within them[5]. Cyberspace is also understood as

1 G. Pilarski, *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020, p. 22.

2 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, no. 5, p. 229.

3 Ibidem, p. 230.

4 *Cyber Security Strategy for Germany 2021*, https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4&utm [access: 31.05.2025].

5 *Cybersecurity: A Generic Reference Curriculum*, eds. S.S. Costigan, M.A. Hennessy, Kingston 2016, p. 7.

a space for processing and exchanging information, created by ICT systems and sets of cooperating IT devices and software that enable the processing, storage, transmission, and reception of data through telecommunications networks. This includes appropriate end-user devices designed for direct or indirect connection to the network, along with the connections between them and their interactions with users[6]. The 2015 Cybersecurity Doctrine of the Republic of Poland describes cyberspace as a battlefield characterised by features that are particularly attractive from the perspective of conducting military operations. It enables the rapid exertion of influence on an adversary located at a significant distance, without exposing soldiers to direct physical risk[7].

With the advent of the 21st century, an increasing number of national armed forces have recognised the possibility of conducting warfare in the virtual domain, which is now regarded as a sixth operational space – alongside land, air, sea, outer space, and the electromagnetic spectrum[8]. It is often noted that any future large-scale global conflict – commonly referred to as World War III – is likely to begin in cyberspace[9].

What types of cyber threats must military operations address today? Among them, particular attention is given to threats targeting a state's critical infrastructure, which is managed through information systems. Deliberate attacks on communication systems that ensure the effective functioning of national security management, defence, and protection subsystems – as well as support systems related to the economy and society – may pose serious risks to national stability. Another vulnerable target in cyberspace includes ICT service providers and operators. Disruptions to their operations, particularly interruptions in service continuity, can hinder the functioning of both public institutions and private sector entities, affecting citizens directly.

Cyberspace operations have become an integral component of contemporary political and military crises and conflicts, often manifesting in

6 R. Janczewski, *Cyberprzestrzeń – część teatru działań hybrydowych*, „Przegląd Sił Zbrojnych" 2019, no. 2, p. 34.

7 See more: *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015.

8 M. Wrzosek, *Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka*, „Kwartalnik Bellona" 2016, no. 4, p. 44.

9 Ibidem, p. 43.

hybrid forms. Such actions have been observed in Ukraine, Libya, and areas controlled by the so-called Islamic State. A distinct category of external cyber threats is cyber espionage, which involves the use of specialised tools to gain access to sensitive data essential for the functioning of state structures. These activities are carried out by foreign intelligence services as well as non-state actors, including terrorist, criminal, and ecological organisations[10]. This paper aims to examine the evolution, role, and strategic significance of military operations in cyberspace, using selected national examples.

Information Superiority in Cyberspace

Universal digitization and automatic transmission of information in command and control systems of means of destruction make cyberspace the main information channel, and the Internet is a global area of information resources for commands and staffs conducting military operations.

According to many experts, a defining feature of modern armed forces is not only the possession of automated command systems, but also the ability of soldiers to locate, process, and transmit information through digital networks to subordinate units and command structures. These systems and networks are operated by personnel using electronic devices and platforms, which today form a fundamental operational domain for contemporary militaries. Information resources are transmitted as „signals" within the digital environment, making them a key target for potential adversaries[11].

Cyberspace has long been an area of interest for military specialists dealing with new technologies. The possibilities of the Internet were quickly noticed by the military and used as a new dimension of military operations. The activities of „knowledge warriors" or „cyber warriors" – as soldiers and military employees are colloquially referred to who acquire information, process it and distribute it – are becoming a common phenomenon in the army. Analytical teams using open sources of information are being created, methods and techniques for segregating information, searching for it and processing it are being developed. Reconnaissance and intelligence specialists

10 Ibidem, p. 50–51.
11 Ibidem, p. 53.

are increasingly using the Internet for the purpose of infiltrating the armies of other countries, and even deliberately disrupting the operation of electronic devices and systems in the armed forces of a potential enemy[12].

The conclusion that emerges from these considerations is that military experts remain divided on the interdependence between operations conducted in cyberspace and those within the electromagnetic spectrum. As a result, scientific discourse presents arguments both in favour of and against merging these two domains. Nonetheless, a widely accepted perspective recognises cyberspace and the electromagnetic spectrum as two distinct yet equally important operational environments. What remains indisputable is the close correlation between contemporary military activities conducted in both spheres[13].

This section explains the concept of electronic warfare. The armed forces extensively utilise the electromagnetic spectrum for purposes such as communication, weapon control, intelligence, surveillance, navigation, and force protection. Electronic warfare plays a vital role in all military operations, with all service components incorporating and integrating it into operational structures to support mission objectives. It is closely coordinated and synchronised with kinetic firepower to disrupt enemy operations and prolong their decision-making process. Electronic warfare contributes to the protection of forces by defending friendly electromagnetic communication and non-communication systems. It also enhances situational awareness, target development and acquisition, battle damage assessment, and overall protection by enabling the identification, location, and exploitation of enemy emitters. Moreover, it supports counter-command and control measures by disrupting, degrading, and neutralising enemy communication tools such as radios, radar systems, and navigation technologies[14].

Three main areas define electronic warfare: electronic support, electronic attack, and electronic protection. Electronic countermeasures within this domain may be offensive or defensive in nature. Offensive actions are typically initiated by friendly forces and include jamming enemy radar and command

12 See more *Pracowite trolle Putina... na cyberwojnie*, https://www.angora.com.pl/spis.php?w=16&y=2015&utm [access: 31.05.2025].

13 M. Wrzosek, op. cit., p. 52.

14 Z. Haig, *Electronic Warfare in Cyberspace*, „Security and Defence Quarterly" 2015, no. 2, p. 23–32.

systems, deploying anti-radiation missiles to suppress enemy air defence, applying deception techniques to mislead enemy intelligence, surveillance, and reconnaissance systems, and using directed energy weapons to disable enemy equipment or capabilities. Defensive countermeasures aim to protect personnel, infrastructure, and operational capabilities, and include methods such as the use of expendables like chaff, flares, and active decoys; radar jammers; towed decoys; infrared countermeasure systems; and jammers that counter radio-controlled improvised explosive devices[15].

The essential purpose of cyber electromagnetic activities is to ensure the integration and synchronisation of cyberspace operations, electronic warfare, and spectrum management operations. Such coordination is intended to produce complementary and reinforcing effects across these domains. In contrast, uncoordinated activities can result in operational conflicts and mutual interference between different components or with other spectrum users. Cyber electromagnetic activities, therefore, encompass cyberspace operations, electronic warfare, and spectrum management functions. In view of the technical and organisational interdependencies between electronic warfare and signals intelligence, cyber electromagnetic operations additionally include signals intelligence as a core element[16].

During the Combat Engineer and Logistics 2025 conference, organised by Defense Leaders, in response to my question regarding the protection of the Eastern Flank, the answer emphasized the combined importance of cybersecurity and electronic warfare. As a result, computer viruses and logic bombs designed to disable enemy systems have become part of the arsenal used not only in military information warfare. Efforts have also been undertaken to develop the use of high-intensity electromagnetic pulses capable of destroying the structures of integrated circuits and permanently damaging computers and other electronic equipment. In addition, research programs have been initiated in laboratories aimed at producing bacterial strains that feed on materials used in the manufacture of electronic circuits[17].

15 Ibidem.

16 Ibidem.

17 P. Sienkiewicz, *Wojna informatyczna*, Computerworld, 31.03.1997, http://www.computerworld.pl/news/291172_2/WOJNA.INFORMATYCZNA.html [access: 26.10.2016].

As previously noted, information warfare is often defined as the totality of offensive and defensive actions necessary to achieve an information advantage over an adversary and to accomplish the intended military and political objectives. The core of such military operations lies in destroying or degrading the value of the opponent's information resources and the systems they use, while simultaneously ensuring the security of one's own information assets and the systems that support them. According to Miron Lakomy, military operations in cyberspace were initiated as early as the mid-1990s[18]. When discussing military operations in cyberspace, it is important to note the establishment of the National Cryptology Center (NCK), an institution responsible for cybersecurity. The Center was created by Order No. 10/MON of 29 April 2013, which established and granted a statute to this state budget unit. Its primary objective was to enhance the security of information processed within the cyberspace of the Ministry of National Defense[19].

Another significant step was Decision no. 17/MON of 5 February 2019 concerning the appointment of the Plenipotentiary of the Minister of National Defense for the establishment of cyberspace defence forces. The plenipotentiary's primary task was to analyse the formal and legal regulations as well as the organisational framework of the Ministry of National Defense in the field of cyberspace security as an operational domain, with consideration for the responsibilities of the Minister of National Defense as defined by law. Additional duties included coordinating actions aimed at establishing the Cyberspace Defence Forces Inspectorate based on the Cyber Operations Centre, coordinating projects related to the creation of cyberspace defence forces, and supervising the proper execution of tasks essential to achieving operational readiness by these forces[20]. The system of ongoing cyberspace security management, developed within the newly formed structure of the cyberspace defence forces, enables the reporting of information on threats and

18 See more M. Lakomy, *Cyber Threats at the beginning of the 21st Century*, „Przegląd Zachodni" 2013, no. 2.

19 J. Świątkowska, I. Albrycht, D. Skokowski, *National Cyber Security Organisation: Poland*, Tallinn 2017, p. 7.

20 Decyzja Nr 17/MON Ministra Obrony Narodowej z dnia 5 lutego 2019 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw utworzenia wojsk obrony cyberprzestrzeni, Dz. Urz. MON 2019, poz. 23.

vulnerabilities, continuous response, as well as the analysis and correlation of activities.

The Polish Armed Forces are a fundamental element of the state's defense system, which must also be focused on effective actions in cyberspace, just as effective actions are in the air, on land and at sea[21]. The tasks of the armed forces in cyberspace encompass the development of operational capabilities, the decryption of foreign military communications, and the protection of their own IT systems and digital resources. They also include combating the sources of cyber threats through active defense and offensive operations, as well as restoring the efficiency and functionality of cyberspace assets. Military deterrence, the defense of networks and information systems, and the planning of the use of civilian sector resources for cooperation with NATO and the EU are equally important responsibilities. In the context of cyber warfare and cyber conflict, the armed forces are expected to conduct military operations specifically tailored to the virtual domain. Additionally, in the area of cyberspace, the Military Counterintelligence Service (SKW) and the Military Intelligence Service (SWW) are tasked with combating cybercrime, cyberterrorism, and cyberespionage. Their duties also include conducting cyber intelligence activities and maintaining close cooperation with NATO and the European Union.

Combat operations in cyberspace are characterised by a high degree of secrecy, which enables a wide range of activities supported by advanced technologies and specialised knowledge. As a result, even states or entities with limited military potential can effectively conduct operations and achieve both political and military objectives[22]. Cryptography has emerged as a new and essential technology in military operations conducted in cyberspace. It serves as a critical and effective component of the protective shield safeguarding strategic assets against cyberattacks. This protection encompasses physical

21 *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/ [access: 1.06.2025].

22 J. Rivera, *Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk*, [in:] *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, eds. M. Maybaum, A.-M. Osula, L. Lindström, Tallinn 2015, p. 8–17.

infrastructure, digital resources, and tools that enable the secure exchange and storage of information.

Military Operations in Cyberspace: The U.S. Armed Forces Perspective

Military operations conducted by the United States Army can be illustrated using the Air Force as an example. The Department of Defense (DoD) defines cyberspace as a global domain within the information environment (IE), consisting of interdependent networks of information technology infrastructures and the data contained within them. This includes the internet, telecommunications networks, computer systems, and embedded processors and controllers[23].

According to Joint Publication (JP) 3-12 „Joint Cyberspace Operations", cyberspace operations refer to the employment of cyberspace capabilities with the primary objective of achieving effects in or through cyberspace. These operations encompass military, intelligence, and routine business activities conducted by the DoD in cyberspace. Military cyberspace operations involve the use of cyberspace capabilities to generate effects that support missions across both physical and virtual domains[24].

Cyberspace operations are categorised into three main types. Offensive Cyberspace Operations are designed to project power through the application of force in and via cyberspace. These are authorised similarly to operations in traditional physical domains. Defensive Cyberspace Operations aim to protect DoD and allied cyberspace and consist of both passive and active defence measures conducted within and outside the Department of Defense Information Network (DODIN). DODIN Operations involve designing, building, configuring, securing, operating, maintaining, and sustaining DoD communications systems and networks throughout the entire DODIN infrastructure[25].

23 *Joint Publication 3-12, Cyberspace Operations*, 8 June 2018, p. I-1, https://irp.fas.org/doddir/dod/jp3_12.pdf [access: 1.06.2025].
24 Ibidem, p. I-2.
25 Ibidem, p. II-3.

In 2012, the DoD initiated the development of the Cyber Mission Force (CMF) to carry out its core cyber missions. The CMF comprises 133 specialised teams. Cyber National Mission Teams are tasked with national defence responsibilities, including monitoring adversary activities, blocking cyberattacks, and manoeuvring in cyberspace to counter hostile actions. Cyber Combat Mission Teams conduct military cyber operations in support of combatant commands. Cyber Protection Teams defend DoD information networks, safeguard critical missions, and prepare cyber forces for engagement. Cyber Support Teams provide analytical and planning support to both National Mission and Combat Mission Teams[26].

Other key institutions within the DoD and the Intelligence Community play supporting or collaborative roles in cyberspace operations. The National Security Agency (NSA), co-located with United States Cyber Command (USCYBERCOM) at Fort Meade, Maryland, plays a central role, especially given the dual-hatted position of the NSA Director, who also leads USCYBERCOM. The NSA's primary responsibilities include providing information assurance for national security systems and conducting signals intelligence (SIGINT)[27]. The Defense Information Systems Agency (DISA) ensures command-and-control capabilities and provides a globally accessible enterprise information infrastructure in direct support of joint warfighting operations. The Director of DISA is responsible for addressing critical DODIN infrastructure issues and also serves as the commander of the Joint Force Headquarters-DODIN (JFHQ-DODIN), which oversees the daily operations and active defence of DoD networks[28]. The Assistant Secretary of Defense for Cyber Policy (ASD-CP), a position established under Title 10 U.S.C. § 138, operates within the Office of the Secretary of Defense. This office is responsible for overseeing DoD cyber policy and supervising the budgetary review of cyber-related activities. The ASD-CP also serves as the Principal Cyber Advisor[29].

26 Ibidem, p. II-7.
27 Ibidem, p. II-8.
28 Ibidem, p. II-9.
29 Ibidem, p. II-10.

Conclusions

Cyberspace has become a fully recognized domain of military operations – just as important as land, sea, air, or outer space. As noted in the introduction, the ability to operate effectively in this environment is now a key element of military strategy. From the perspective of 2025, it is clear how much has changed in this field over the past decade. This article presented the U.S. military approach to cyberspace operations, with particular focus on the Air Force and the Cyber Mission Force. It also highlighted how differently Russia views and uses cyberspace – not only as a battlefield, but also as a tool for influence and disinformation.

Today, after more than ten years of dynamic development, we can reflect on these processes from a historical perspective. The establishment of specialized commands, the expansion of cyber defense structures, and growing international cooperation – including NATO and European Union initiatives – show that Western countries have taken this challenge seriously. EU funding has also played an important role in building cyber defense capabilities. If European forces are to be well prepared for future threats, they must not only develop their own technologies and structures, but also understand how their adversaries think and act. The fundamentally different approach to cyberspace demonstrated by Russia is not only an operational challenge – it is also a cognitive one.

Bibliography

Cyber Security Strategy for Germany 2021, https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4&utm [access: 31.05.2025].

Cybersecurity: A Generic Reference Curriculum, eds. S.S. Costigan, M.A. Hennessy, Kingston 2016.

Haig Z., *Electronic Warfare in Cyberspace*, „Security and Defence Quarterly" 2015, no. 2.

Janczewski R., *Cyberprzestrzeń – część teatru działań hybrydowych*, „Przegląd Sił Zbrojnych" 2019, no. 2.

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/ [access: 1.06.2025].

Lakomy M., *Cyber Threats at the beginning of the 21st Century*, „Przegląd Zachodni" 2013, no. 2.
Pilarski G., *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020.
Pracowite trolle Putina... na cyberwojnie, https://www.angora.com.pl/spis.php?w=16&y=2015&utm [access: 31.05.2025].
Rivera J., *Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk*, [in:] *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, eds. M. Maybaum, A.-M. Osula, L. Lindström, Tallinn 2015.
Sienkiewicz P., *Wojna informatyczna*, Computerworld, 31.03.1997, http://www.computerworld.pl/news/291172_2/WOJNA.INFORMATYCZNA.html [access: 26.10.2016].
Świątkowska J., Albrycht I., Skokowski D., *National Cyber Security Organisation: Poland*, Tallinn 2017.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, no. 5.
Wrzosek M., *Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka*, „Kwartalnik Bellona" 2016, no. 4.

Operacje militarne w cyberprzestrzeni przed 2022 rokiem: założenia strategiczne i doktryny

Streszczenie

Cyberprzestrzeń stała się kluczową domeną operacyjną współczesnych sił zbrojnych, oprócz lądu, morza, powietrza i przestrzeni kosmicznej. Artykuł dotyczy sposobu prowadzenia operacji wojskowych w cyberprzestrzeni przez Stany Zjednoczone Ameryki oraz Federację Rosyjską. Autorka skoncentrowała się na obowiązujących doktrynach, strukturach organizacyjnych i realnych możliwościach operacyjnych. Wskazała zasadnicze różnice w definiowaniu cyberprzestrzeni oraz jej wykorzystywaniu do celów ofensywnych, defensywnych i strategicznych. Szczególną uwagę poświęciła roli walki radioelektronicznej oraz integracji zdolności cybernetycznych z planowaniem militarnym w szerszym ujęciu. W artykule uwzględniła również konsekwencje tych różnic dla NATO i Unii Europejskiej, zwłaszcza w kontekście narastających napięć oraz ewoluującego charakteru zagrożeń hybrydowych.

Słowa kluczowe: cyberprzestrzeń, operacje wojskowe, wojna elektroniczna, strategia