The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

Received: *October 4, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 2, 2025* | **Published Online:** *March 21, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2025.3.4.23

Systematisation of capabilities for confrontation in cyberspace on the geopolitical stage: experience in the establishment of cyber units and the specifics of their functioning

Yurii Kliat
Candidate of Technical Sciences, Associate Professor
Head of the Central Research Institute of the Armed Forces of Ukraine
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: klyatt@ukr.net
ORCID:0000-0002-8267-3748

Oleksandr Deineha
Doctor of Military Sciences, Professor
Chief Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28B, Kyiv, Ukraine
e-mail: davdoma@gmail.com
ORCID: 0000-0002-2371-3252

Oleh Nechaiev
First Deputy Commander
Special Operations Forces of the Armed Forces of Ukraine
e-mail: o26811650@gmail.com
ORCID: 0009-0001-2839-2830

Denis Molchanov
Researcher
Research Laboratory Department of Military Training
State University “Kyiv Aviation Institute”
03048, Medova Street 1, Kyiv, Ukraine
e-mail: mdbua2@gmail.com
ORCID: 0009-0007-9268-2764

Abstract. The article presents the results of a systematisation of capabilities for confrontation in cyberspace on the geopolitical stage, specifically focusing on the experience of establishing cyber units and the characteristics of their functioning. The purpose of the article is to analyse and generalise the capabilities of the world’s armed forces to conduct confrontation in cyberspace (ensuring state cyber defense) at the geopolitical level, in order to introduce contemporary development trends of cyber units into the process of acquiring combat and special capabilities of the prospective Cyber Forces of the Armed Forces of Ukraine. During the research, general scientific methods of analysis

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

and generalization were applied, which in combination made it possible to obtain a systematisation of capabilities for conducting armed confrontation in cyberspace on the geopolitical stage. The method of analysis was used to examine in detail the experience of establishing cyber units within military institutions at the geopolitical level, as well as the specific features of their functioning. The method of generalisation made it possible to identify common characteristics of the analysed experience of creating cyber units in the armed forces of the world and the peculiarities of their functioning, enabling a transition "from the particular to the general." The main scientific result of the study is the developed systematisation of capabilities for conducting armed confrontation in cyberspace on the geopolitical stage, namely the experience of establishing cyber units and the specifics of their functioning. A distinctive feature of the proposed systematisation is that it consists of two parts: the first highlights the experience of establishing and the functional characteristics of capabilities of the world's leading armed forces, while the second covers other armed forces that are at the stage of acquiring capabilities for conducting cyber confrontation. The practical value of the obtained scientific result lies in the possibility of implementing modern development trends of cyber units in the process of acquiring combat and special capabilities of the prospective Cyber Forces of the Armed Forces of Ukraine. The prospects for further research in the direction outlined in the article include the introduction of advanced information technologies, as well as artificial intelligence technologies, into the activities of cyber confrontation forces and means of the Security and Defence Sector of Ukraine.

Keywords: operation, artificial intelligence, cyber actions, cyber defence, cyber intelligence, cyber influence, cyber protection, cyberspace, control, cybersecurity, cyber warfare, information security, information space, system stability, information technologies.

Introduction

Recent studies in the field of acquiring and developing capabilities for the prospective Cyber Forces of the Armed Forces of Ukraine (AFU) to conduct operations in cyberspace (ensuring the cyber defence of the state), for example [1], have developed and substantiated recommendations for acquiring such capabilities within the security and defence sector of Ukraine as a whole and the AFU in particular. One of the proposed approaches to the acquisition and development of cyber warfare capabilities is to take into account the experience of capabilities for conducting cyber confrontation (cyber defence, cyber intelligence, and cyber influence) on the geopolitical stage. In particular, there is a need to analyse and generalise the best international practices in the establishment and functioning of cyber units within defence institutions of various states, including their performance of assigned tasks.

The capability-based defence planning process has been examined in studies [2–5], which provide a detailed overview of general approaches to the acquisition and development of combat and specialised capabilities. At the same time, cyberspace, due to its dependence on the rapid development of modern computer and information technologies, requires separate strategies and approaches for capability development in order to conduct effective confrontation within this domain.

Certain scholars whose research focuses on cybersecurity and cyber defence, for example [6], argue that in contemporary geopolitics all wars (military conflicts) involving technologically advanced states can be considered cyber wars to some extent. Such conflicts are characterised by a prolonged preparatory phase, often lasting several years, during which the vulnerability of the target state is systematically created or exploited prior to an attack. In particular, it is common for cyber confrontation or its individual components (cyber intelligence, cyber defence, and cyber influence) to be conducted over a long period before the active phase of a conflict begins, albeit in a more covert manner than during the overt phase of hostilities.

In the armed forces of leading states on the geopolitical stage, units responsible for conducting

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

operations in cyberspace have been functioning for a considerable period of time. In the defence institutions of many other countries, however, such units are still in the process of acquiring and developing their capabilities. Nevertheless, the experience gained from the formation of cyber units and the particular features of their functioning provides invaluable insights, revealing best practices that can be implemented in the process of acquiring and developing the capabilities of the prospective Cyber Forces of the AFU.

The purpose of this article is to analyse and generalise the capabilities of the world's leading armed forces in conducting cyber confrontation (ensuring cyber defence of the state) on the geopolitical stage, with the aim of incorporating modern trends in the development of cyber warfare units into the process of acquiring combat and specialised capabilities for the prospective Cyber Forces of the Armed Forces of Ukraine.

Methodological Framework

The methodological foundation of the study is based on the application of general scientific methods of analysis and synthesis to the investigation of capabilities for conducting cyber confrontation (ensuring the cyber defence of the state) on the geopolitical stage. Collectively, these methods allow for the systematisation of experience in the establishment and operational characteristics of cyber units in the armed forces of leading states, with the aim of integrating modern trends in the development of cyber warfare units into the process of acquiring combat and specialised capabilities for the prospective Cyber Forces of the Armed Forces of Ukraine (AFU).

The essential capabilities required for the prospective Cyber Forces of the AFU to conduct cyber confrontation (implementation of military measures for cyber defence) include [7]:

capacity to conduct informational defence measures for the state;

establishment of a cyber defence system to operate in the information environment, including cyberspace;

capability to ensure effective cyber protection of the national information infrastructure (critical information infrastructure), including the conduct of preventive measures for detecting, responding to cyberattacks and cybersecurity incidents, and mitigating their effects under conditions of enemy cyber intelligence and intensive cyber influence (cyberattacks);

capability to conduct cyber reconnaissance and counter-reconnaissance within information and telecommunication networks and systems of state, private, and military significance (including critical infrastructure) of the adversary, to obtain information on the enemy's cyber infrastructure, its purpose, location, technological processes, vulnerabilities, and to establish covert control, intercept, and decrypt command, resource data, and information;

capability to plan and conduct coordinated demonstrative cyber operations (cyber influence) in cyberspace to prevent the escalation of armed conflicts, deter aggression, and repel cyber hostilities;

capability to organise and conduct cyber operations (cyber influence, cyberattacks) using all types of cyber weapons, including seizure or neutralisation of enemy systems, causing damage (cascading effects), disrupting the functioning of critical and information infrastructure, while simultaneously concealing traces of own activities in cyberspace;

application of hardware-software cybersecurity complexes, cyber defence tools, and cyber weapons to achieve objectives in cyber confrontation.

The above-mentioned capabilities for cyber confrontation were initially declared in 2021, whereas the Draft Law on the Cyber Forces of the AFU [8] was submitted at the end of 2024. Therefore, the analysis and synthesis of the capabilities of leading armed forces worldwide in conducting cyber confrontation (ensuring state cyber defence) on the geopolitical stage, aimed at integrating modern trends into the development of cyber warfare units for the acquisition of combat and specialised capabilities by the prospective Cyber Forces of the AFU, remains a highly relevant and significant scientific task.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

Results and Discussions

At the current stage of armed confrontation in cyberspace during contemporary military conflicts, the main trends in the functioning (task execution) of cyber warfare units (cyber defence, cyber intelligence, and cyber influence) are [9]:

1. Trend towards conducting complex, multi-stage full-spectrum cyber operations, driven by the overall development of applied computer information technologies, the increased general level of cybersecurity in computer information systems and networks, as well as the rising demands for the results of such operations.

2. Trend towards the use of DDoS attacks as one stage of a cyber operation to enhance its effect or to mislead the adversary. The isolated use of such attacks has ceased to be as effective as it was in earlier stages of the development of military cyber units on the geopolitical stage.

3. Achievement of cyber operation objectives typically relies on a cyber-social chain (phishing, social engineering, man-in-the-middle attacks, etc.). At present, humans (officials) remain the weakest link in the functioning of computer systems and networks, whereas discovering previously unknown vulnerabilities in cyber defence systems is becoming increasingly difficult.

4. Continuous cyber operations by states occur both in peacetime and during military conflicts (local wars and armed conflicts). Typically, cyber intelligence begins several years before the onset of a conflict, while the execution of active destructive cyber influence precedes the kinetic phase (mass missile and air strikes, ground operations) by 1–2 days.

5. Pattern of malware reuse: harmful software that has previously succeeded is often modernised, modified, and reapplied (e.g., Agent.btz forming the basis of Uroborus, WannaCry forming the basis of NotPetya).

6. Confirmed trend regarding the People's Republic of China: primarily conducts cyber intelligence (without destructive cyber influence), with new evidence indicating a high degree of stealth, allowing years of undetected access to confidential information of rival states on the geopolitical stage.

7. Hypothetical cooperation (experience exchange) exists between the cyber warfare units of the Democratic People's Republic of Korea and the russian federation concerning the development of cyber warfare methods and tactics.

8. The United States Cyber Command is one of the few cyber warfare units globally that officially acknowledges the cyber operations it has conducted.

To implement modern trends in the development of cyber warfare units in the process of acquiring combat and specialised capabilities of the prospective Cyber Forces of the Armed Forces of Ukraine, it is necessary to analyse and summarise the capabilities of leading world armies in conducting cyber counteraction (ensuring the cyber defence of the state) on the geopolitical stage.

In the United States – the U.S. Cyber Command (USCYBERCOM), established in May 2010, performs functions of planning, coordination, and conducting military operations in cyberspace [10]. USCYBERCOM is the main structure coordinating cyber operations in the interests of U.S. national security, reporting to the Department of Defense and operating in conjunction with the NSA (National Security Agency). Its main tasks include the protection of the Department of Defense and the national information infrastructure, conducting digital intelligence, and carrying out defensive and, upon decisions of the senior command, offensive cyber operations. USCYBERCOM is considered the leading cyber warfare unit in the world, setting trends for other nations. USCYBERCOM is organised into the following components:

U.S. Army Cyber Command – operation of computer networks, cyber protection of army information and communication systems, cyber intelligence at the ground operations level;

U.S. Fleet Cyber Command / United States Tenth Fleet – cyber protection of naval information systems, cyber security of surface and subsurface platforms, intelligence against maritime threats;

Air Forces Cyber / Sixteenth Air Force – computer network security, management of aviation

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

information flows, and countering threats in the air domain;

Marine Corps Forces Cyberspace Command – cyber protection of Marine Corps systems, support for tactical cyber operations.

In the People's Republic of China (PRC) – the Network Systems Department of the Strategic Support Force of the People's Liberation Army integrates all available cyber unit capabilities regarding information and cyber warfare, controls digital operations, security, and cyber intelligence. Its structure includes twelve bureaux, a computing centre, and three research institutes, divided according to functions [11]:

network and critical infrastructure defence – ensuring the reliability of military communications and protection against attacks;

cyber and signals intelligence – systematic collection of technical information from open and closed sources, including electronic intelligence;

scientific and technical development – working on protection tools and threat analysis instruments, cryptography, and algorithms;

electronic warfare (EW) – integrating electronic warfare with the digital systems of adversaries.

A distinctive feature of the PRC's cyber units' organisational structure is that these bureaux are specifically focused on states or state blocs (USA, Japan, Taiwan, Western countries, russia, and other Asian countries), the comprehensive study of which in cyber terms is the primary activity of the Network Systems Department. The command hierarchy and organisational structure of the PRC's cyber units are shown in Figure 1 [13].

<table>
<tr><td colspan="8">Central Military Commission of the Communist Party of China</td><td>Other departments</td></tr>
<tr><td colspan="8">Army Strategic Support Force</td><td rowspan="3">Other cyber warriors including the Militia, Internet commentators and opinion leaders, and cyber police</td></tr>
<tr><td colspan="2">Aerospace System Department</td><td colspan="2">Network System Department</td><td colspan="2">Electronic/ Electromagnetic System Department</td><td colspan="2">Military Intelligence Department</td></tr>
<tr><td colspan="7">12 bureaux under the Third Department of the People's Liberation Army's General Staff Department</td><td>Others</td></tr>
<tr><td>Unit 61398 (the U.S. as the main target)</td><td>Unit 1486 (western countries as the main target)</td><td>Unit 661419 (Japan as the main target)</td><td>Unit 78020 (Southeast Asia as the main target)</td><td>Unit 61726 (Taiwan as the main target)</td><td>Unit 61786 (Russia and Central Asia as the main target)</td><td>Unit 69010 (Central Asia and Southeast as the main target)</td><td>Other units</td><td>(Such as information war force under the headquarters, Base 311)</td><td></td></tr>
</table>

Figure 1. Structure of units conducting armed cyber operations in the PRC

The cyber units shown in the figure above maintain close links with civilian organisations (Chinese state-owned companies, academic institutions) to coordinate IT resources in the field of national security. China's strategy emphasises proactive cyber defence of its own cyber infrastructure, cyber intelligence on rival states on the geopolitical stage, and the expansion of technological capabilities [12].

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

In the russian federation, there is no single publicly known central command for units dedicated to conducting armed cyber operations, as exists in the USA or China. However, there are several structures performing cybersecurity, cyber intelligence functions, and offensive cyber operations in the interests of the state, namely [13]:

Main Centre for Special Technologies of the General Staff of the Armed Forces of the russian federation – directly linked to the prominent cybercriminal group Sandworm and considered responsible for cyberattacks on Ukraine's energy sector in 2015, 2016, and 2022, as well as for the NotPetya cyberattack campaign;

Federal Security Service (FSB) – responsible for oversight of cybersecurity in state computer networks and counterintelligence in cyberspace.

Additionally, cyber units exist within the Foreign Intelligence Service of the russian federation.

Moreover, several advanced persistent threat (APT) cybercriminal groups are associated with russian cyber units:

APT Sandworm – targeting critical infrastructure;

APT Fancy Bear – active against political, military, and media targets;

APT Turla – conducting sophisticated attacks with prolonged covert presence in networks;

APT Nobelium (also known as APT29) – focusing on government networks.

North Korea (DPRK) does not publish official details about its cyber structures. Analysts from international IT companies and intelligence agencies have identified that state-directed activities are often coordinated through the APT Lazarus Group – the country's most prominent cybercriminal organisation, conducting operations in digital espionage, financial intrusions, and malware deployment. Among the most well-known cyberattacks attributed to the APT Lazarus Group are: cyber influence on the information infrastructure of the USA and South Korea through a series of DDoS attacks in 2009; cyberattacks on several South Korean media outlets and financial companies on 20 May 2013; and cyber influence using the WannaCry malware in 2017.

Israel has a well-developed national cyber defence system (including cyber intelligence and cyber protection) that incorporates both defensive and offensive components [14]. One of the main units for conducting armed cyber operations is Unit 8200, an intelligence-oriented cyber unit within the country's armed forces intelligence department. Unit 8200 primarily conducts signals intelligence, decryption of intercepted data, cyber reconnaissance, and, according to expert assessments, participation in cyber operations.

In Iran, similarly to the russian federation, there is no central cyber command like that of the USA. Nevertheless, cyber operations are coordinated by several institutions, including [15]:

Islamic Revolutionary Guard Corps (IRGC) – a key actor with its own cyber and electronic warfare capabilities (units);

Ministry of Intelligence and Security (MOIS) – conducting intelligence and cyber operations, including via affiliated APT-type cybercriminal groups;

Basij Cyber Council – volunteer organisations for covert cyber operations, operating under the control of the IRGC.

This approach to conducting armed cyber operations allows for leveraging the hybrid nature of cyber actors to achieve intelligence and offensive objectives, maximising the effect of available capabilities.

The capabilities of the most prominent geopolitical cyber actors have been analysed above, and their capacities are summarised in Table 1.

At the same time, other nations' armed forces are also developing cyber operational capabilities. Examples of such states on the geopolitical stage are provided below.

Belgian Cyber Force is part of the Belgian Armed Forces, established in 2022 to counter digital threats of both defensive and intelligence nature. The unit works on protecting IT infrastructure of state and military systems, threat analysis, countermeasures against disinformation, and, under

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

political directives, cyber operations. Its command cooperates with academic institutions and the private sector on encryption and cryptography.

Table 1. Cyber operational capabilities of the most prominent geopolitical cyber actors

Country	Main Cyber Structure	Status	Main Functions	Sources
USA	U.S. Cyber Command (including cyber commands of the armed services)	Military-state	Network defence, cyber intelligence, defensive and authorised offensive operations	[10]
China	Department of Network Systems, Strategic Support Force of the People's Liberation Army	Military	Protection of military networks, cyber intelligence, electronic warfare	[11, 12]
russian federation	Main Directorate of the General Staff, Federal Security Service, APT groups (Sandworm, Fancy Bear, etc.)	State agencies, "unofficial"	Intelligence, influence, digital attacks	[13]
Israel	Unit 8200	Military/Intelligence	Cyber intelligence, defence, cyber operations, cooperation with security agencies	[14]
DPRK	Lazarus Group and others	Opaque	Cyber espionage, financial operations	(general assessments)
Iran	IRGC, MOIS, Basij Cyber Council	Hybrid	Cyber defence, cyber intelligence, offensive cyber operations	[15]

The Estonian Cyber Command is a formal structure within the Estonian Defence Forces, responsible for the protection, defence, and potentially offensive cyber operations in the interests of the state. Its main tasks include ensuring the functioning of IT services, threat monitoring, information security analysis, strategic communications, and the training of specialists in this field.

In Lithuania, the Cyber Defence Command (LTCYBERCOM) was established in 2025 as part of the national armed forces to provide operational management of cyber defence, plan cyber operations, analyse threats, and ensure the resilience of communication and information systems. The command comprises a headquarters, an IT service, and a battalion supporting strategic communications.

The Polish Cyberspace Defence Forces constitute a specialised component of the national military, designed to secure military computer systems and networks. Its responsibilities include military cyber defence, intelligence, and potentially defensive and proactive measures, with coordination through the National Cybersecurity Centre.

The Italian Network Operations Command is a military formation responsible for information security, network operations, and cyber defence. The unit performs defensive functions (protection of networks and IT infrastructure) as well as analytical and operational tasks within the cyber environment.

Thus, although the EU as a collective bloc does not have a single military cyber command, many NATO and EU member states are establishing national cyber defence structures and integrating them into the Alliance's collective defence system. NATO regards cyberspace as a domain of defence and armed operations, conducting large-scale cyber defence exercises with member states and partners.

From a military perspective, the experiences of South American and African countries in developing capabilities for conducting armed cyber operations are also noteworthy.

In South America, cyber defence and cybersecurity develop unevenly. Research indicates that some countries (e.g., Brazil, Argentina, Colombia, Mexico) have national cybersecurity strategies and have begun forming corresponding structures within their governments and militaries. These models

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

often combine state Computer Emergency Response Teams (CERTs), police cybercrime centres, and military cyber defence components. For instance, Colombia has established the Joint Cyber Command of the General Command of the Armed Forces in response to the need to protect critical infrastructure and defence systems [16].

On the African continent, approaches to cybersecurity are emerging through both multi-stakeholder policies and military/security structures. Evidence shows that South Africa is one of the regional leaders, with specialised structures for cybersecurity that include military components of information warfare and cyber operations, focused on protecting national interests. Nigeria is also developing a Cyber Warfare Command within its armed forces to counter cyber threats and offensive cyber operations. Egypt integrates a cyber component into its C5ISR commands to protect military and state systems. In Morocco, military cyber support centres and training facilities operate for regional cooperation. Additionally, many African countries have national cybersecurity strategies encompassing military, civil, and private sectors, although the level of development varies significantly [17].

A summary of the experiences in establishing cyber units and their operational features within the armed forces of countries at the stage of developing capabilities for conducting armed cyber operations is presented in Table 2.

In the Armed Forces of Ukraine, cyber operational capabilities should be consolidated within the prospective Cyber Forces of the Armed Forces of Ukraine. Taking into account the experience in establishing and operating cyber units in the armed forces of other states on the geopolitical stage is a crucial condition for rapidly acquiring the necessary combat and specialised capabilities, as well as achieving operational readiness of this branch of the Ukrainian Armed Forces.

Table 2. Summary of the experience in establishing cyber units and their operational characteristics in the armed forces of countries at the stage of developing capabilities for conducting armed cyber operations

Country	Main Cyber Structure	Status	Primary Cybersecurity Body
Belgium	Cyber Command	Military	Cyber defence, intelligence, cyber counterintelligence
Estonia	Cyber Command	Military	Defence, cyber operations
Lithuania	Cyber Defence Command	Military	Planning, protection, threat analysis
Poland	Cyberspace Defence Forces	Military	Military cyber defence
Italy	Network Operations Command	Military	Defence/cyber operations
Argentina	Joint Cyber Defense Command	Military/State	Protection of military information resources, CERT
Colombia	Joint Cyber Command	Military/State	Protection of critical information infrastructure
Africa (South Africa, Nigeria, Egypt, Morocco)	Various military cyber units	Military/State	Computer network protection, cyber intelligence

Conclusion

Thus, this article presents the results of the analysis and synthesis of capabilities for conducting cyber operations (ensuring state cyber defence) on the geopolitical stage. Collectively, these results allow for the systematisation of the experience in establishing and operating cyber units within the armies of the world, with a view to implementing contemporary trends in the development of military units and cyber operations subunits in the process of acquiring combat and specialised capabilities for the prospective Cyber Forces of the Armed Forces of Ukraine. A prospective direction for further research on the development of combat and specialised capabilities of the Armed Forces of Ukraine in conducting cyber operations is the integration of advanced information technologies, including

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

artificial intelligence technologies, into the activities of the cyber operations forces and assets within Ukraine's security and defence sector.

Recommendations

The article may be useful for cybersecurity specialists, officials in military command bodies, military units and subunits involved in the preparation and conduct of cyber operations, academic and research staff, as well as cadets, students, and trainees studying issues related to cybersecurity, cyber operations, and the experience of establishing and operating active cyber units on the geopolitical stage.

Conflict of Interest

The author of the article is a member of the editorial board. To avoid a conflict of interest, the editorial process was conducted by Oleh Semenenko.

References

1. Horbatiuk, V., Horhulenko, V., Horhulenko, V., Dobrovolskyi, Yu., & Samsonenko, M. (2025). Recommendations on the Implementation of Defence Planning Measures for Acquiring and Developing Capabilities by the Prospective Cyber Forces of the Armed Forces of Ukraine Based on the DOTMLPFI. *Military Science*, *3* (2), 137–150. https://doi.org/10.62524/msj.2025.3.2.10.
2. Nalyvaiko, A. D., Polyayev, A. I., & Nalyvaiko, L. P. (2019). Theoretical Foundations of Building a Functional Model of the Defense Planning Process for Defense Forces. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2* (66), 35–41. https://doi.org/10.33099/2304-2745/2019-2-66/35-41.
3. Nalyvaiko, A. D. (2024). Justification of Directions for Improving Strategic Planning in the Defense Sector. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine*, *1* (80), 27–33. https://doi.org/10.33099/2304-2745/2024-1-80/27-33.
4. Deniezhkin, M. M., Nalyvaiko, A. D., & Polyayev, A. I. (2017). Features of Defense Planning in NATO Member States Based on Capabilities. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2* (60), 34–38. https://doi.org/10.33099/2304-2745/2017-2-60/34-38.
5. Fediienko, O. P. (2024). Modern Trends in Normative Support for Institutional Formation of Cyber Forces (Cyber Troops): The Experience of Some NATO Countries. *Information and Law, 1* (48), 150–161. https://doi.org/10.37750/2616-6798.2024.1(48).300800.
6. Kohut, Yu. I. (2023). *A new type of hybrid war as a threat to the national security of states*. Consulting company «SIDKON»; Publishing house «DAKOR»
7. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"* (473/2021). https://zakon.rada.gov.ua/laws/show/473/2021#Text.
8. *Draft Law on Cyber Forces of the Armed Forces of Ukraine.* https://itd.rada.gov.ua/billinfo/Bills/Card/45453.
9. Horhulenko, V. A. (2024). Cyber Warfare in Modern Conflicts: Advanced Experience, Trends, and Development Patterns. *Modern Information Technologies in Security and Defense, 2* (50), 11–28. https://doi.org/10.33099/2311-7249/2024-50-2-11-28.
10. Tkachuk, N. A. (2024). US experience in creating and developing Cyber Command. *Information and law*, *1* (48), 139–149. https://doi.org/10.37750/2616-6798.2024.1(48).300798.
11. Tsung-Han Wu, Chia-Ling Hung. (2021). *Cyber Warfare Capabilities of the PLA Strategic Support Force.* Institute for National Defence and Security Research. https://indsr.org.tw/uploads/enindsr/files/202206/64b998f3-d906-46a4-b78e-08c06eb28c3e.pdf

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

12. *Key international and Ukrainian cybersecurity news in September 2024.* (2024). https://www.rnbo.gov.ua/ua/Diialnist/7027.html
13. *Pentagon chief orders cessation of offensive cyber operations against Russia.* (2025). https://ms.detector.media/kiberbezpeka/post/37611/2025-03-03-golova-pentagonu-doruchyv-prypynyty-nastupalni-kiberoperatsii-proty-rosii-nyt
14. *Army beefs up cyber-defense unit as it gives up idea of unified cyber command.* (2017). https://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command
15. *Iran's cyber capabilities and hackers.* (2025). https://www.ferner-alsdorf.com/irans-cyber-capabilities-and-hackers
16. *Cybersecurity in Latin America and the Caribbean: the state of readiness for the defense of cyberspace.* (2015). https://wjpcenter.org/wp-content/uploads/2023/09/Cybersecurity-in-Latin-America-and-the-Caribbean.pdf
17. *The evolving cybersecurity frontier in Africa*. (2025). https://africandefence.co.uk/the-evolving-cybersecurity-frontier-in-africa

Систематизація спроможностей з протиборства у кіберпросторі на геополітичній арені: досвід створення кіберпідрозділів та особливості їх функціонування

Юрій Клят
кандидат технічних наук, доцент
начальник Центрального науково-дослідного інституту Збройних Сил України
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: klyatt@ukr.net
ORCID:0000-0002-8267-3748

Олександр Дейнега
доктор військових наук, професор
головний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: davdoma@gmail.com
ORCID: 0000-0002-2371-3252

Олег Нечаєв
перший заступник командувача Сил спеціальних операцій ЗС України
Сили спеціальних операцій ЗС України
e-mail: o26811650@gmail.com
ORCID: 0009-0001-2839-2830

Денис Молчанов
Науковий співробітник науково-дослідної лабораторії
кафедри військової підготовки
Державний університет "Київський авіаційний інститут"
03048, вулиця Медова 1, Київ, Україна
e-mail: mdbua2@gmail.com
ORCID: 0009-0007-9268-2764

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

Анотація. Стаття висвітлює результати систематизації спроможностей з протиборства у кіберпросторі на геополітичній арені, а саме досвіду створення кіберпідрозділів та особливостей їх функціонування. Метою статті є аналіз та узагальнення спроможностей армій світу з ведення протиборства у кіберпросторі (забезпечення кібероборони держави) на геополітичній арені для впровадження сучасних тенденцій розвитку підрозділів кіберборотьби у процес набуття бойових і спеціальних спроможностей перспективних Кіберсил Збройних Сил України. Під час проведення дослідження було використано загальнонаукові методи аналізу та узагальнення, які у сукупності дозволили отримати систематизацію спроможностей з ведення збройного протиборства у кіберпросторі на геополітичній арені. Методом аналізу було розкрито деталі досвіду створення кіберпідрозділів у військових відомствах на геополітичній арені, а також особливостей їх функціонування. Метод узагальнення дав змогу отримати загальні ознаки проаналізованого досвіду створення кіберпідрозділів в арміях світу, та особливостей їх функціонування – перейти “від одиничного до загального”. Основним науковим результатом проведеного дослідження є сформована систематизація спроможностей з ведення збройного протиборства у кіберпросторі на геополітичній арені, а саме досвіду створення кіберпідрозділів та особливостей їх функціонування. Особливістю отриманої систематизації є те, що вона складається з двох частин: перша висвітлює досвід створення та особливості функціонування спроможностей передових армій світу, а друга – інших, тих, які перебувають на етапі набуття спроможностей з ведення кіберборотьби. Практичною цінністю отриманого наукового результату є можливість впровадження сучасних тенденцій розвитку підрозділів кіберборотьби у процес набуття бойових і спеціальних спроможностей перспективних Кіберсил Збройних Сил України. Перспективою подальших досліджень за означеним у статті напрямом є впровадження новітніх інформаційних технологій, а також технологій штучного інтелекту в діяльність сил і засобів кіберборотьби сектору безпеки і оборони України.

Ключові слова: операція, інформаційна безпека, інформаційний простір, інформаційні технології, управління, кібербезпека, кіберборотьба, кібервплив, кібердії, кіберзахист, кібероборона, кіберпростір, кіберрозвідка, стійкість системи, штучний інтелект.