UDC 004.056:343.3
DOI: 10.32518/sals4.2023.192

Соціально-правові студії. 2023. Т. 6, № 4
Social & Legal Studios. 2023. Vol. 6, No. 4

Legal aspects of the cybertechnology development and the cyberweapon use in the state defence sphere: Global and Ukrainian experience

Oleh Semenenko*

Doctor of Military Sciences, Professor
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitroflotskiy Ave., Kyiv, Ukraine
https://orcid.org/0000-0001-6477-3414

Uzef Dobrovolskyi

PhD in Technical Sciences, Associate Professor
National Aviation University
03058, 1 Liubomyr Huzar Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-1077-1402

Maryna Sliusarenko

PhD in Technical Sciences, Senior Researcher
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitroflotskiy Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-4165-3908

Ihor Levchenko

PhD in Military Sciences, Associate Professor
Odesa Military Academy
65009, 10 Fontanska Doroha Str., Odesa, Ukraine
https://orcid.org/0000-0003-3428-4761

Serhii Mytchenko

Adjunct
National Defence University of Ukraine
03049, 28 Povitroflotskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-3711-2033

Abstract. The research relevance is determined by the development of the digital sphere, which entails an increase in the number of cybercrimes and cyberattacks that pose a threat to the security of people and organisations and can lead to serious consequences. The study aims to examine how cyber technologies are formed and developed, as well as how they are used in the field of state defence in Ukraine and some European Union countries, namely Germany, France, the United Kingdom, and Indonesia. In the course of the study, were used structural-functional and dialectical methods, the method of synthesis, logical and comparative analysis, and the method of generalisation. It is established that cybertechnologies are gaining more and more development both in the world and in Ukraine, and cyberweapons, due to their effectiveness and negative consequences, are equated with methods of mass destruction. That is why the issue of cyber defence is one of the main challenges of our time. Ukraine needs to adopt international experience to successfully formulate policies and create its own legal and organisational framework for cybersecurity. Using the experience of other countries, Ukrainian experts will be able to improve their technologies and strategies, strengthen defences in the information space, and develop new advanced defence systems. The importance of the National Coordination Centre for Cybersecurity should be emphasised. The body's work is focused on ensuring coordination of the activities of the

Suggested Citation

Article's History: Received: 19.08.2023 Revised: 16.11.2023 Accepted: 23.12.2023

Semenenko, O., Dobrovolskyi, U., Sliusarenko, M., Levchenko, I., & Mytchenko, S. (2023). Legal aspects of the cybertechnology development and the cyberweapon use in the state defence sphere: Global and Ukrainian experience. *Social & Legal Studios*, 6(4), 192-199. doi: 10.32518/sals4.2023.192.

*Corresponding author

national security and defence entities of Ukraine in the implementation of the cybersecurity strategy in the country and on improving the efficiency of the public administration system in the formation and implementation of the state policy in the field of cybersecurity. The study is practically important, since all the theoretical provisions, conclusions and recommendations can be used by legislators and other specialists to improve the system of legal guarantees of cybersecurity in the field of defence of the State

Keywords: virtual space; digital development; computer attacks; information wars; national security

Introduction

The problems related to cybersecurity have proved to be the most urgent and, at the same time, the most difficult to solve in the field of national security and defence for all nations around the world. Information and cyber elements play a systemic role in all forms of armed struggle, including military operations. This is especially true in times of crisis when the number of cyberattacks, and cyber incidents is growing significantly. Along with the digital revolution and the development of information technology, the number of cyber threats is growing. Every aspect of society's existence, the efficiency with which vital infrastructure, including public administration, as well as security and military operations, functions, are targets of cyberattacks, which in turn is truly creating a new security environment. The relevance of the problem is driven by efforts to develop cyberspace capabilities to ensure the protection of the state.

Currently, due to insufficient study of the legal and regulatory framework for the use of cyber technologies in Ukraine, as well as the lack of effective and accurate methods for detecting and countering cyber-attacks, several problems may arise, including disruption of critical infrastructures, information operations that can be used to manipulate public opinion, disinformation and destabilise the socio-political situation, and leaks of confidential information that can be used against the national interests of the state (Sopilko & Rapatska, 2023).

According to research by A. Pekhnik and Yu. Zavgorodnya (2021), cybertechnologies are gaining ground both globally and in Ukraine. This is noticeable not only in the commercial sphere but also in the political sphere (election processes, terrorism). New threats and trends in cybercrime are on the rise. As noted by L. Samchuk and D. Nastachenko (2023), cyberspace is a new environment created for the exchange of information and the use of cyber weapons due to the rapid development of information technology and modern digital space. According to Ukrainian legislation, "cyberspace" is an environment (virtual space) that facilitates public relations and/or communication and is created when compatible (linked) communication systems are in operation and electronic communications are available via the Internet and/or other means of international data transmission.

According to a study by Yu. Kohut (2020), the development of Ukrainian cybersecurity legislation is gradual, considering international legal documents and cybersecurity strategies of other countries. The Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine" (2017) is the most significant legal act, as it defines not only the legal and organisational framework for ensuring the protection of the vital interests of a person and a citizen but also the interests of society and the state in cyberspace. It defines the main tasks, directions, and guiding principles of state policy in this area, the powers of state bodies, enterprises, institutions, organisations, and citizens in this area, as well as the main areas of coordination of their actions to ensure cybersecurity. This law is a comprehensive piece of special legislation relating to cybersecurity.

According to L. Veselova (2021), to successfully formulate an appropriate policy and build its system of legal and organisational protection of cybersecurity, in particular in the context of hybrid warfare, Ukraine needs to acquire international experience in the field of administrative and legal protection of cybersecurity. This experience should be applied in practice. To ensure the success and effectiveness of legal support for cybersecurity, simultaneous actions are needed to develop national legislation appropriate to address the challenges of hybrid warfare in this area and to cooperate with professional international institutions to ensure cybersecurity. According to research by Yu. Chernysh *et al.* (2023), cooperation at both the national and international levels is needed to protect against various cyber threats. Cyberattacks are becoming a growing threat to Ukrainian and global organisations. As noted in the research results of A. Biliuha (2021), given the powerful military potential, cyber weapons are gradually becoming more destructive and dangerous than traditional weapons and military equipment.

Currently, the issues of problems faced by the information and communication technology professions in Ukraine, their current state, and further prospects for the development of cybersecurity professions have not been sufficiently studied. Considering the aforementioned, the study aims to determine the legal aspects of the formation, development, and implementation of cyber technologies in the field of state defence in the example of Ukraine, Germany, France, and the United Kingdom. To achieve this goal, the following tasks are set: to study the stages of formation and legal aspects of the development of cyber technologies in Ukraine, to study international experience in the field of cyber defence, and to highlight the advantages of foreign cyber defence strategies that can have a positive impact on improving the national strategy.

Materials and methods

To study in more detail the issues of formation and development of cyber technologies, as well as their application in the field of state defence, theoretical research methods were used, namely analysis, synthesis, as well as dialectical and structural-functional methods.

Using the structural-functional method, the authors examine the main concepts of this study, namely, "cyberspace", "cyberattack", "cybersecurity", "cyber-defence", identify the legal aspects of cyber technology development, study the activities of cyber security agencies, and consider the experience of using cyberweapons in the defence sector of such countries as Ukraine, Germany, France, the United Kingdom, and Indonesia. The essence of the concept of cyberweapons is studied based on national and international documents. The guidelines for the application of international law in cyber warfare are analysed. The authors identify

devices, mechanisms, equipment, or software used to carry out cyberattacks, as well as their main purposes and possible consequences of use. The stages of development of cyber technologies in the field of security and defence are studied, which helps to understand new challenges and adapt to them. The authors analyse the technical experience of using cyber weapons on the example of the Stuxnet virus. The factors that led to the emergence of such threats as cyberwar, cybercrime, cyberterrorism, and cyberespionage are identified. Using the dialectical method, the research, and views of other scholars on this issue were studied and a unified view of the development and use of cyber technologies to protect the state and citizens in various spheres of life was formed.

The methods of analysis and synthesis were primarily used in the study. The subject of this study was divided into several parts to study the problem in more detail. In the first part, the authors identified the peculiarities of cybersecurity in Ukraine and analysed the historical and legal aspects of the development and establishment of the cyber defence institution. The authors identified the system of cybersecurity actors and the peculiarities of their legal status. The forms of ensuring information security were highlighted. The authors also analysed the legislative framework of Ukraine in the field of cyber defence, analysed the activities of the State Centre for Cyber Defence, the National Coordination Centre for Cybersecurity, the National Security and Defence Council of Ukraine, and the governmental computer emergency response team Computer Emergency Response Team of Ukraine (CERT-UA), and examined their main functions and tasks. The second part of the study analysed the experience of European countries (Germany, France, the United Kingdom, and Indonesia). The main document designed to ensure cybersecurity in the UK, as well as the activities of the National Cyber Security Centre (NCSC), are analysed. The structure of state bodies in the field of cybersecurity in Germany is studied, and the German Cybersecurity Strategy and the activities of the National Cybersecurity Council are analysed. The main regulatory acts of France in the field of cyber security – the National Digital Security Strategy and the White Paper on Defence and National Security – are studied.

The authors highlight the positive aspects of other countries' experience in applying cyber technologies in the field of state defence and identifies what Ukraine needs to pay attention to for successful policymaking and the creation of an organisational and legal framework. The second method – synthesis – was used to formulate recommendations for improving Ukrainian legislation in the field of cyber defence and to organise all the information received into a single work.

Results

With the development of technology, cyberspace is becoming a new and equally important area where countries compete to protect their national interests. It also includes international terrorist organisations and transnational organised crime.

One of the main goals of Ukraine's national security policy is to create a cybersecurity system and ratify the Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cyber Security of Ukraine" (2017). The basic law in the field of cybersecurity defines the concepts of critical infrastructure facilities, information infrastructure facilities and mechanisms for protecting such facilities, the idea of creating a national cybersecurity system and its components, and the powers and coordination of cybersecurity actors. Part 1 of Article 8 of the Law of Ukraine No. 2163-VIII states that the national cybersecurity system of Ukraine consists of a set of security entities and related political, scientific, technical, informational, educational, organisational, legal, operational, investigative, intelligence, counterintelligence, defence, engineering and technical nature, as well as measures of cryptographic and technical protection of national information resources and cyber defence of critical information infrastructure.

The creation of the State Service for Special Communications and Information Protection (SSSCIP), which includes the State Centre for Cyber Defence (SCCD), on 1 July 2015 is one of the priorities of the national cybersecurity system. The State Centre for the Protection of Information and Telecommunication Systems of the State Service for Special Communications was the basis for its establishment (Horun, 2023). Effective cyberspace operations are essential for the fulfilment of national security tasks. The effectiveness of actions is determined by the need to create a cyber-defence system as soon as possible, which focuses on the preparation and implementation of defence measures, as well as the necessary capabilities for the development of forces and weapons in cyberspace, which will ensure the creation of the necessary potential in the field of defence of the state as a whole and other component of the security sector.

Thus, as a result of the development of IT technologies, the widespread use of the Internet and the illegal activities of cyber criminals, a whole new class of weapons known as "cyberweapons" has emerged. Cyberweapons have evolved into a first-strike weapon that aims to deliberately interfere with another state's ability to command, operate, and influence targets for destruction or control, including not only the military domain, but also other infrastructures, communications, governance systems, a state's population, economy, and leadership (Rid & McBurney, 2012). Due to their constant functional modification and improvement, no universal definition of "cyberweapons" exists in the global practice. Nevertheless, the essence of this phenomenon is explained in several national and international documents. In the Guidelines for the Application of International Law in Cyber Warfare, an international scientific group stated that cyber weapons are an offensive tool for cyber warfare. Their intended use and design imply the possibility of damage, destruction and serious consequences when used. Cyber tools can be any apparatus, mechanism, equipment, or software used to carry out cyberattacks. There are stages in the genesis of cyber technologies in the security and defence sector that help to understand and adapt to new challenges (Table 1).

Table 1. Stages of development of cyber technologies in the field of state defence

Stages	Main actions	Expected results
Stage 1 (up to 2014). Beginning of cyber capability development	Establishment of core cyber defence units, as well as the creation of fundamental cyber defence strategies and policy programmes	Formation of the first departments and units in the field of cyber defence

Table 1, Continued

Stages	Main actions	Expected results
Stage 2 (2014-2018). Cyber capability improvement and expansion	Formation of specialised research centres; cooperation with foreign partners; increase in the number of cybersecurity specialists	Development of in-house cyber capabilities to counter cyber attacks
Stage 3 (2018-2020). Integrated cyber defence system implementation	Creation of a system for countering new types of cyberattacks and development of improved monitoring and response systems	Creating cyber defence systems capable of detecting and countering cyber-attacks in real-time
Stage 4 (2020-2023). Development of cyber weapons and cyber operational capabilities	Development of attacking cyber capabilities, development of cyber operational capabilities, development of coordination with other types of cyber weapons	Formation of a new cyber weapons capability to protect national interests
Stage 5 (after 2023). Integrating cyber technologies into the overall defence strategy	Integration of cyber defence and cyber-attacks into a single defence strategy, development of a system for the use of cyber weapons in various cyber conflict scenarios	Creation of an adaptive cyber defence strategy that can be used in conjunction with traditional military means

Source: compiled by the authors

It is necessary to objectively assess the conflict in cyberspace, find solutions to countering cyber weapons and transition to the principles of active defence, considering the experience of leading states and international organisations. In this regard, it is necessary to emphasise the importance of the National Coordination Centre for Cybersecurity, as it is a functional unit of the National Security and Defence Council of Ukraine. That body aims to ensure national security and defence coordination in implementing the country's cybersecurity strategy and to improve the efficiency of the public administration system in formulating and implementing the state policy in the field of cybersecurity. Furthermore, the State Centre for Cyber Defence of the State Service for Special Communications and Information Protection of Ukraine has a governmental group for responding to computer emergencies, CERT-UA (Computer Emergency Response Team of Ukraine). The main task of CERT-UA is to methodically protect the activities of state institutions and citizens of Ukraine from unauthorised intrusion into the country's cyberspace, counteract cyber weapons. However, this body cannot conduct investigations or prosecute cybercriminals, as it does not have the powers of an investigative body (Trofymenko *et al.*, 2019).

Studying European countries, the United Kingdom's experience is crucial, as it is currently the world's leader in cybersecurity. The National Cyber Security Strategy is the main document designed to guarantee cybersecurity in the UK. It is particularly important to note that the National Cyber Security Centre (NCSC) was established on 1 October 2016 to implement the Strategy. To keep the nation safe online, the NCSC offers governments, companies, and the general public a rare opportunity to successfully collaborate on cybersecurity. Overall, a careful analysis of the UK National Cyber Security Strategy reveals that there are many intriguing and emerging aspects of the strategy that require further research. Some advantages of the Strategy should be highlighted, namely (Condruţ, 2023):

- major effort in public awareness on protection from possible violations of rights in the area under study;
- official interpretation of certain concepts in the field of cybersecurity (e.g., cyber defence, active cyber defence), definition and consolidation;
- detailed description of directions and stages of implementation of innovations in the field of cybersecurity;
- designation of specific areas of employee training, as it is impossible to guarantee cybersecurity without appropriate staff support.

Germany demonstrates the complex structure of government agencies in the field of cybersecurity. The state devotes considerable effort to supporting cyber defence. Furthermore, Germany actively uses international cooperation, which contributes to the development of local laws and technologies, as well as to the faster and more efficient detection of threats in this area. Another positive aspect is that the number of initiatives aimed at implementing state policy in the field of cybersecurity is constantly increasing. Similar to the UK, Germany adopted the German Cybersecurity Strategy in 2011. According to this strategy, the federal government responds to threats in the following strategic areas by implementing measures based on existing institutions, depending on the level of threat. One of the main tools for preventing cybersecurity is measures to identify and eradicate the constructive causes of crises. To implement these measures, the National Centre for Cyber Defence and the National Council for Cybersecurity were established, with the main goals (Schallbruch & Skierka, 2018):

- protecting the largest critical information infrastructures;
- improving the IT security system of the Federal Republic of Germany;
- strengthening IT security in public administration;
- maximising operational cooperation of all government agencies and strengthening coordination of measures to protect against IT incidents;
- forming a successful campaign to combat cybercrime;
- forming global and European cooperation in the field of cybersecurity;
- using reliable information technologies.

Considering the experience of France, it is worth noting the National Digital Security Strategy of 2015 and the White Paper on Defence and National Security of 2008 as the main regulatory acts that define the strategic guidelines of the state security policy. Therefore, the White Paper includes the following as the most likely threats to the territory of

France and the European Union: organised crime, terrorism, ballistic missile use, natural hazards, epidemiological problems in large cities and hidden immigration, mass attacks on information networks; espionage and strategic influence. The Strategy has five goals, including adaptation to digital transformation and aims to combat new threats associated with the evolution of digital technologies (Darwish & Romaniuk, 2021).

According to Law No. 3 of 2002 on National Defence of the Republic of Indonesia, the objectives of national defence are to protect national security from all threats, both military and non-military, and to preserve and protect the sovereignty and territorial integrity of the unitary state. The country's ability to resist, act and restore cyber defence must be strengthened due to non-military threats, especially those arising in cyberspace. This is done in support of the National Cybersecurity Strategy implemented by the Ministry of Communications and Information Technology (Inggarwati *et al.*, 2020).

Technical experience in the use of cyberweapons is already available: the Stuxnet virus was created in the United States of America. In the future, the status of cyber weapons in the digital space will only grow. It is believed that the Stuxnet cyber virus was used in one of the most famous cyber-attacks of all time. In 2010, this system code was used to compromise the SCADA1 systems that operate more than a thousand uranium enrichment centrifuges manufactured by Siemens, based in Natanz, Iran. The attack rendered the company's centrifuges unusable. In addition, the virus behaved in a way that prevented centrifuge operators from detecting any anomalies during the operation of the device. The malicious code also altered the equipment's operating parameters, making the process uncontrollable and leading to the physical failure of the centrifuges (Collins & McCombie, 2012). This incident received significant attention, although the United States has not yet officially acknowledged its involvement. Many other countries have also experienced some form of attack on infrastructure and websites operated by governments and non-governmental organisations. These include both highly developed cyber nation-states (the United States, the United Kingdom, Israel, South Korea, and China) and less developed cyber nation-states. All these examples demonstrate the growing importance of cyberspace in international relations and the need for legal regulation among the subjects of this legislation. It is important to remember that technologies are developing much faster than the rules for their use. As a result, national laws relating to cyberspace should be consolidated, and global harmonisation of these standards is needed.

Unlike previous cyberattacks, cyber warfare is now considered a major threat to state and national security. In addition, many intelligence services of countries use the Internet for cyber espionage, information gathering, hacking into computer systems, sabotage, and economic espionage. Due to the development of new technologies, the level of cyber warfare is constantly increasing. I. Zhaborynska (2018) argues that China is the world's leader in cyber warfare. Some states started to address cyber warfare, allocating the necessary funds to organise defence systems, and supporting special units whose main task is to improve the country's security on the Internet and protect against attacks. Hostile cyber-attacks have become more frequent and sophisticated, and some of them may come from within rather than without.

Discussion

Nowadays, hackers can attack both individuals and entire states. Scientists have started to use the phrase "cyber weapons", comparing them to weapons of mass destruction due to their effectiveness and possible consequences. Therefore, cybersecurity is one of the main development vectors. It is impossible to refute the conclusions of L. Kovács (2018) that states should have adaptive and dynamic cybersecurity plans to respond to attacks in cyberspace that are constantly evolving and changing. Even though cyberspace has no physical borders, countries often develop in-house cybersecurity strategies based solely on their ideals and perceptions of security. This leads to the existence of different approaches to ensuring security in the information space in different countries. The results of the study showed that initially, the cybersecurity strategies of European countries (e.g. Germany, France) were developed from the perspective of the information society and its security forecasts, while other countries, such as the United States and Singapore, took a different approach to developing cyber defence strategies, focusing on critical information infrastructures and their security issues.

The study by A. Klimburg (2012) outlines the key objectives of a national cybersecurity strategy and highlights the following factors: national security and cybersecurity strategy should be linked; conflicts may arise between military and civilian approaches to a national cybersecurity strategy; the development and implementation of the strategy should take into account various national characteristics; the national cybersecurity strategy should be allocated appropriate resources and objectives should be quantified; the process of developing the human resources required to build cybersecurity is often more complex than expected.

The study results of H.S. Lallie *et al.* (2021) note the many instances of fraud since the outbreak of the COVID-19 epidemic, where individuals or organisations impersonate government agencies (such as WHO) and organisations (such as supermarkets, and airlines), are noteworthy. These scams target both the millions of people who work from home and the general public. Remote employment has exposed people to certain security issues and challenges in the information space that the public or businesses have never experienced before. Cybercriminals have taken advantage of this situation to intensify their attacks using classic deception that exploits people's increased levels of stress, anxiety, and worry. Critical infrastructure, including medical services, has also been targeted.

Cyberspace and related technologies are one of the most important sources of power in the third millennium. Y. Li and Q. Liu (2021) highlight the concept of power dispersal, a phenomenon caused by the characteristic features of cyberspace, including low entry costs, anonymity, vulnerability, and asymmetry. This means that governments have to share power in this area with other actors, such as individuals and private enterprises. The government will not lose its national security as a result of this phenomenon. Numerous methods can be used to assess this effect. Today, the possibility of a decline in the quality of life is a challenge to national security. It is no longer possible to define national security in terms of military issues, and internal and external borders. Cyber threats are complex, irregular, and extremely harmful as they involve infrastructure and networks that are highly vulnerable. Individuals and businesses are also susceptible to their negative impact. Government action alone is not

enough to counter these threats. Effective bilateral cooperation is needed between the ruling elite and the private sector, which has a common interest in dealing with them. These threats cannot be contained by traditional means, such as the use of military and police force.

However, the authorities now face additional challenges in the field of state protection. As J. Cao *et al.* (2021) note, organised crime and terrorist groups have become active participants in cyberspace due to their low cost of entry, anonymity, unpredictable geographic location, dramatic impact, and lack of public transparency. These factors have led to threats such as cyberwarfare, cybercrime, cyberterrorism, and cyberespionage. The aforementioned study results are noteworthy as they distinguish cyber threats from traditional national security threats, which are more covert and primarily affect identified governments and nations in a particular region. As such, national defence in the traditional sense is under attack and becomes less effective in this area. Several scenarios could lead to serious and sometimes widespread physical or economic damage. For example, a virus could attack financial documents in the economic system or disrupt the stock market; it could also send the incorrect command, causing a power plant to shut down; it could even interfere with air traffic control, leading to air crashes.

Following L.B.S. Putra and R. Sutanto (2022), cyber defence operates at multiple levels, from individual to collective to government. Sectors that control vital infrastructure, including energy, transport, the financial system, defence security and other public services. Failure of electronic systems in these sectors can cause financial losses, reduced public confidence in the government, disruption of public order and other problems. This risk reflects the requirements for reliable cyber defence in one country. According to research, cyber defence institutions currently support IT in general, rather than being focused on supporting targeted national defence requirements. While efforts to establish cyber defence institutions are ongoing, they mainly consist of tying cyber defence responsibilities and functions to the current structure. Reliable availability and accessibility of cyberspace are essential for the success of conventional military operations in other domains. The sphere of IT is now institutionalised as a policy within the North Atlantic Treaty Organisation.

The conclusions of M. Górka (2023) on how cyber technologies have changed traditional ways of thinking, opening up new avenues for action, are noteworthy. All of this supports the expansion of the definition of "cyber warfare" beyond the conventional interpretation to include conflicts related to information warfare. The term "cyber warfare" indicates that this phenomenon makes it possible to use cyber solutions alongside military operations, even instead of conventional warfare. This new form of armed conflict has changed the traditional definition of war. Therefore, the meaning of terms such as attack, defeat and battlefield is gradually changing. Attacking an enemy's strategic cyber structures, network, information, and communication can lead to victory.

In the long history of military technology advancing new operational and tactical concepts, cyber warfare is yet another form of conflict. According to J. Arquilla and D. Ronfeldt (1997), many experts initially described cyber warfare as the acquisition and exploitation of enemy intelligence. Modern armed forces are increasingly dependent on secure, instantaneous flows of vast amounts of information, and any disruption in these flows could very soon have catastrophic consequences for combat readiness. An enemy force would be unable to fight a battle or a military campaign as it would be unable to maintain control of its units and track their location or status.

Therefore, in this context, the state policy on cybersecurity should aim to achieve significant results and be aimed at forming a protected national segment of cyberspace; avoiding interference of foreign states in internal affairs and their encroachment on information resources; increasing the state's defence capability in cyberspace; and reducing the vulnerability of cyber defence objects.

Conclusions

The study revealed that the Law of Ukraine "On the Principles of Ensuring Cybersecurity of Ukraine" is the most significant legal act in the area under study, as it defines both the legal and organisational basis for guaranteeing the protection of vital interests of a person and a citizen, as well as public and state interests in cyberspace. It identifies the main tasks, directions, and guiding principles of state policy in this area, the powers of state bodies, enterprises, institutions, organisations, citizens, and citizens, as well as the main areas of coordination of their actions to ensure cybersecurity. This act is a comprehensive piece of special legislation relating to information security. Cybersecurity is one of the main challenges as cyber weapons have become a first-strike weapon, which aims to deliberately interfere with the ability to control and influence the objectives of another state to defeat or control, including not only the military sphere but also other infrastructures, communications, governance systems, the population, and the economy.

Analysing the experience of other countries in the use of cyber technologies in the field of state defence, it is necessary to conclude that Ukraine needs to consider international experience to successfully formulate policies and create its legal and organisational framework for cybersecurity protection, especially in the case of hybrid warfare. By using the experience of other countries, Ukrainian cybersecurity and defence experts will be able to gain new knowledge and competencies that they can use to improve their technologies and strategies. Foreign expertise will allow Ukraine to strengthen its defence and cybersecurity, as other countries may have more experience in dealing with cyber threats and developing advanced defence systems. Tapping into foreign expertise would also reduce dependence on imported software and hardware, which could increase domestic autonomy in the cybersecurity and defence sectors. Ukraine's international relations can be strengthened through cooperation on joint cybersecurity and defence projects and programmes with foreign partners. Ukraine can increase its capacity to develop new cyber technologies and creative solutions in the field of security and defence by adopting foreign experience.

The scientific novelty of the study is determined by the fact that the process of formation and application of cyber technologies in the field of state defence was studied in detail, and recommendations for improving the national policy and organisational and legal framework in the field of cybersecurity were identified. Prospects for further research are to develop a system for improving the legal support for cyber defence in the area of the private life of citizens.

Acknowledgements

None.

Conflict of interest

None.

References

[1] Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is coming! In J. Arquilla, & D. Ronfeldt (Eds.), *Athena's Camp: Preparing for conflict in the information age* (pp. 23-60). Santa Monica: RAND Corporation.

[2] Biliuha, A.D. (2021). Cyber weapons: Modern threats to national security and countermeasures. *Science and Defense*, 2, 42-49. doi: 10.33099/2618-1614-2021-15-2-42-49.

[3] Cao, J., Ding, D., Liu, J., Tian, E., Hu, S., & Xie, X. (2021). Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. *Information Sciences*, 548, 69-84. doi: 10.1016/j.ins.2020.09.046.

[4] Chernysh, Yu.O., Maltseva, I.R., & Shtonda, R.M. (2023). Cyber protection in organizations of various spheres of activity. In *General scientific approaches to knowledge in the different sciences: Proceedings of the XV International scientific and practical conference* (pp. 17-19). Vilnius: InterSci.

[5] Collins, S., & McCombie, S. (2012). Stuxnet: The emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, 7(1), 80-91. doi: 10.1080/18335330.2012.653198.

[6] Condruț, C. (2023). Comparative analysis of strategic cyber security focus areas – United Kingdom, Estonia, Romania. *Romanian Intelligence Studies Review*, 29, 33-61.

[7] Darwish, A., & Romaniuk, S.N. (2021). Cyber security in the French Republic. In S.N. Romaniuk, & M. Manjikian (Eds.), *Routledge companion to global cyber-security strategy* (pp. 62-72). London: Routledge. doi: 10.4324/9780429399718-7.

[8] Górka, M. (2023). A definitional framework for cyber warfare. The Ukrainian aspect. *Polish Political Science Yearbook*, 51. doi: 10.15804/ppsy202272.

[9] Horun, O. (2023). The foreign experience of legal security and features of the creation of cybertroops on the example of some NATO states. *Scientific Bulletin of the International Humanities University. Series: Jurisprudence*, 64, 33-37. doi: 10.32841/2307-1745.2023.64.7.

[10] Inggarwati, M.P., Celia, O., & Arthanti, B.D. (2020). Online single submission for cyber defense and security in Indonesia. *Lex Scientia Law Review*, 4(1), 83-95. doi: 10.15294/lesrev.v4i1.37709.

[11] Klimburg, A. (Ed.). (2012). *National cyber security. Framework manual*. Tallinn: NATO CCD COE Publications.

[12] Kohut, Yu. (2020). Legal fundamentals of the formation and development of the state system of cyber-security in Ukraine. *Entrepreneurship, Economy and Law*, 12, 170-174. doi: 10.32849/2663-5313/2020.12.29.

[13] Kovács, L. (2018). National cyber security as the cornerstone of national security. *Land Forces Academy Review*, 23(2), 113-120. doi: 10.2478/raft-2018-0013.

[14] Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, article number 102248. doi: 10.1016/j.cose.2021.102248.

[15] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[16] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. doi: 10.1016/j.egyr.2021.08.126.

[17] Pekhnik, A.V., & Zavgorodnya, Yu.V. (2021). Modern threats of cyber technologies in political process. *Actual Problems of Politics*, 68, 76-82. doi: 10.32837/app.v0i68.1293.

[18] Putra, L.B.S., & Sutanto, R. (2022). Formation of cyber forces for encounter modern warfare and cyber warfare. *International Journal of Research and Innovation in Social Science*, 6(8), 149-152.

[19] Rid, T., & McBurney, P. (2012). Cyber-weapons. *The RUSI Journal*, 157(1), 6-13. doi: 10.1080/03071847.2012.664354.

[20] Samchuk, L.S., & Nastachenko, D.V. (2023). Cyberspace as a result of virtualization. In V.P. Diachuk (Ed.), *Searching for the new meanings of the polycultural world. Post-war dialogue of cultures: Materials of the international scientific and practical conference* (pp. 115-117). Kyiv: National Academy of Managerial Staff of Culture and Arts.

[21] Schallbruch, M., & Skierka, I. (2018). *Cybersecurity in Germany*. Cham: Springer. doi: 10.1007/978-3-319-90014-8.

[22] Sopilko, I., & Rapatska, L. (2023). Social-legal foundations of information security of the state, society and individual in Ukraine. *Scientific Journal of the National Academy of Internal Affairs*, 28(1), 44-54. doi: 10.56215/naia-herald/1.2023.44.

[23] Trofymenko, O., Prokop, Yu., Loginova, N., & Zadereyko, O. (2019). Cybersecurity of Ukraine: Analysis of the current situation. *Ukrainian Information Security Research Journal*, 21(3), 150-157. doi: 10.18372/2410-7840.21.13951.

[24] Veselova, L.Yu. (2021). *Administrative-legal bases of cyber security in the context of hybrid war*. (Doctoral thesis, Odesa State University of Internal Affairs, Odesa, Ukraine).

[25] Zhaborynska, I. (2018). Cyber wars and cyber technologies, their role in politics. In T.V. Honcharuk (Ed.), *Sociocultural and political priorities of the Ukrainian nation in the conditions of globalization* (pp. 491-493). Ternopil: Ternopil National Economic University.

Правові аспекти розвитку кібертехнологій та використання кіберзброї у сфері оборони держави: світовий та український досвід

Олег Михайлович Семененко

Доктор військових наук, професор
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітрофлотський, 28Б, м. Київ, Україна
https://orcid.org/0000-0001-6477-3414

Юзеф Броніславович Добровольський

Кандидат технічних наук, доцент
Національний авіаційний університет
03058, просп. Любомира Гузара, 1, м. Київ, Україна
https://orcid.org/0000-0002-1077-1402

Марина Олександрівна Слюсаренко

Кандидат технічних наук, старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітрофлотський, 28Б, м. Київ, Україна
https://orcid.org/0000-0003-4165-3908

Ігор Славович Левченко

Кандидат військових наук, доцент
Військова академія
65009, вул. Фонтанська дорога, 10, м. Одеса, Україна
https://orcid.org/0000-0003-3428-4761

Сергій Віталійович Митченко

Ад'юнкт
Національний університет оборони України
03049, просп. Повітрофлотський, 28, м. Київ, Україна
https://orcid.org/0000-0003-3711-2033

Анотація. Актуальність дослідження зумовлено розвитком цифрової сфери, що тягне за собою збільшення кількості кіберзлочинів та кібератак, які становлять загрозу безпеці людей та організацій і можуть призвести до тяжких наслідків. Дослідження має на меті дослідити, як формуються та розвиваються кібертехнології, а також як вони використовуються у сфері захисту держави в Україні та деяких країнах Європейського Союзу, а саме Німеччині, Франції, Великій Британії та Індонезії. У процесі дослідження використано структурно-функціональний та діалектичний методи, метод синтезу, логічного та порівняльного аналізу, метод узагальнення. Установлено, що кібертехнології набувають усе більшого розвитку як у світі, так і в Україні, а кіберзброю за ефективністю та негативними питання кіберзахисту – один з головних викликів сучасності.наслідками прирівнюють до методів масового ураження. Обґрунтовано позицію, що Зазначено, що Україні необхідно запозичити міжнародний досвід для успішного формування політики та створення власної правової та організаційної бази кібербезпеки. Виснувано, що, використовуючи досвід інших країн, українські фахівці зможуть удосконалювати свої технології та стратегії, зміцнювати захист в інформаційному просторі, розробляти нові передові системи захисту. Підкреслено важливість Національного координаційного центру кібербезпеки. Робота органу зосереджена на забезпеченні координації діяльності суб'єктів національної безпеки та оборони України щодо реалізації стратегії кібербезпеки в державі та на підвищенні ефективності системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки. Дослідження має практичне значення, оскільки всі теоретичні положення, висновки та рекомендації можуть використати законодавці та інші фахівці для вдосконалення системи правових гарантій кібербезпеки у сфері оборони держави

Ключові слова: віртуальний простір; цифровий розвиток; комп'ютерні атаки; інформаційні війни; національна безпека