INFORMATION SECURITY OF THE DEFENSE FORCES IN UKRAINE: CURRENT STATE AND PROSPECTS

Olha O. Zolotar[1]

Mykola M. Zaitsev[2]

Vitalii V. Topolnitskyi[3]

Kostiantyn I. Bieliakov[4]

Ihor M. Koropatnik[5]

Abstract: The relevance of the article is determined by the fact that security is always one of the priority issues of state policy, and given the fact that the defense forces are an integral part of the state's security, the study of their information security is necessary. The feasibility of this study is confirmed by the fact that in the current conditions of the information society development, information technologies of the Ukrainian defense forces need to adapt to existing challenges and threats in order to ensure adequate protection of information that is of strategic importance to the state and is collected, summarized, stored by the defense forces. The purpose of the article is to identify the problems of information protection of the defense forces in Ukraine, to find areas of their elimination. Formal logical, system structural, comparative legal methods were used to conduct the study. It is noted that by separating the information space and cyberspace, the legislator has complicated the legal regulation of the protection of the state's information space. It is noted that efforts to prevent threats to the information space in Lithuania and Latvia have been consolidated within the structure of the Ministry of Defense. Accordingly, the authors emphasize the need for the optimization of the system of entities

[1] Scientific Research Institute of Informatics and Law at the National Academy of Legal Sciences of Ukraine, Saksahanskyi Street, 110-c, Kyiv, 01032, Ukraine. E-mail: olha.zolotar@tanu.pro

[2] Central Research Institute of the Armed Forces of Ukraine, Povitroflotskyi Avenue, 28-b, Kyiv, 03049, Ukraine

[3] National Defence University of Ukraine named after Ivan Cherniakhovskyi, Povitroflotskyi Avenue, 28, Kyiv, 03049, Ukraine.

[4] Scientific Research Institute of Informatics and Law at the National Academy of Legal Sciences of Ukraine, Saksahanskyi Street, 110-c, Kyiv, 01032, Ukraine

[5] Taras Shevchenko National University of Kyiv, M. Lomonosov Street, 81, Kyiv, 03189, Ukraine

responsible for the protection of the information space, the creation of conditions for public-private cooperation in this area, as in the case of Germany, and the provision of these entities with qualified employees. The results obtained are important for the research, lawmaking and law enforcement activities.

Keywords: information space, cyberspace, telecommunication technology, global information system, state security.

Introduction

The 2030 Agenda for Sustainable Development, adopted by the United Nations, recognizes that the proliferation of information and communication technologies and the global interconnection of networks create significant opportunities to accelerate progress in all areas of human life and bridge the already existing digital divide (Transforming our World…, 2015). Considering this, this agenda calls on every state to take measures aimed at significantly expanding access to information and communication technologies and to strive for universal access to the Internet in the least developed countries (The 2030 Agenda for Sustainable Development, 2015).

Despite the number of benefits associated with the proliferation of information and telecommunications technologies, they threaten the security of the state's information space. This is confirmed by the consequences of the Petya virus attacks, which have increased Ukraine's anti-rating in information security issues and have caused significant damage to European countries. This virus has become a kind of indicator of the status of national and international tools aimed at protecting the information space from existing threats. At the same time, it put on the agenda a number of important tasks, in particular, consolidating the policies of all states in the area of developing high-quality security standards for the information space, software for government structures, creating state agencies responsible for the formation and implementation of policies in this area.

Information space security is a key task for a number of authorities today, including entities belonging to the state's defense forces. In Ukraine, such entities include the Armed Forces of

Ukraine, but in modern conditions, even the information and telecommunication systems of the latter are being attacked from sources geographically located around the world. Thus, according to the Ministry of Defense of Ukraine, in 2019, 52.97% of the attacks were from the Russian Federation, 13.99% from China, 6.50% from the United States, 5.89% from Kazakhstan, 4.31% from Iran, 3.87% from Israel, etc. This confirms that the information and telecommunication systems of the Armed Forces of Ukraine are daily exposed to significant threats, while they belong to the subjects responsible for the state security, which is also a component of information security. Accordingly, in the context of threats both to the security of the information space of the state as an object and to the information and telecommunication system of authorized entities, issues of strengthening the information security of the defense forces are becoming especially relevant. Reznik, O., Olga Getmanets, O., Kovalchuk, A., Nastyuk, V., Andriichenko, N. note that financial, information, military security and others are important and interconnected components of which the state of national security depends in the current context of globalization (Reznik et al., 2020).

It is worth noting that, despite the relevancy of the issue of information space security in the socio-political discourse, many authors point that it is understudied in the scientific literature. M. Nieles, K. Dempsey, V.Ya. Pillitteri define information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to ensure confidentiality, integrity, and accessibility. According to scientists, information is facts or ideas that can be presented (coded) in the form of various forms of data; knowledge (e.g., data, instructions) in any medium or form that may be communication between the entities of the system (Nieles et al., 2017).

O.M. Kosohov, considering information security, substantiates that it is a component of Ukraine's military security since there is a direct dependence on the implementation of Ukraine's most important interests in the military sphere on information threats (Kosohov, 2016). It is worth paying attention to the opinion of E.S. Pelevina who emphasizes the close relationship

between the problem of information security and the concepts of international security and economic globalization. Thus, the key need of the state today is the need to create the conditions necessary for its functioning and development. At the same time, the rapid spread of information and telecommunication technologies and the need to minimize the risks posed by them put the world community at risk of maintaining international security (Pelevina, 2017).

International information security implies the protection of the global information system from terrorist, criminal and military-political threats. The discussion of this issue raised at the Conference on Information Community and Development, held in South Africa in May 1996, led to the adoption in 1998 of the Resolution No. 53/70 Developments in the field of information and telecommunications in the context of international security at the 53rd session of the General Assembly of the United Nations. The above resolution recognized for the first time at the international level the possibility of the negative consequences of the spread and use of information technologies and means (Pelevina, 2017).

The protection of the information space of the state against internal and external threats is usually the responsibility of specially authorized entities. In particular, according to the Concept of Development of the Security and Defense Sector of Ukraine in 2016, ensuring information and cybersecurity is one of the tasks of the security and defense sector (Presidential Decree on the Decision…, 2016a). However, V.Yu. Bohdanovych, B.O. Vorovych and Ye.I. Marko note that foreign experience, particularly that of the USA and Israel, shows that the security and defense sector structure has its own information security system, which has the functions and tasks of identifying and neutralizing information security threats – information security and defense threats (Bohdanovych et al., 2018).

At the same time, information security and cybersecurity cannot be considered to be the sole task of state security and defense authorities since. As Alan Ho Wei Seng points out, the key task is the close cooperation with all actors at the national level and with the competent authorities at the international level on the timely exchange of information on probable threats, search and optimization of areas for the

prevention of threats to information space (Seng, 2016). Moreover, cooperation between the entities of different countries, as well as the latter with international structures, is one of the conditions for their successful activity in any field. The confirmation is the study by O.O. Vakulyk, N.S. Andriichenko, O.M. Reznik, V.V. Volik, K.D. Yanishevska, which emphasizes the need to improve the activities of the entities engaged in the fight against financial crime based on establishing interaction with the authorized bodies at national and international levels (Vakulyk et al., 2019). Thus, considerable attention is paid to the issue of information security in the scientific doctrine; at the same time, we consider it appropriate to disclose the information security of the defense forces of Ukraine in more detail, which will both deepen existing scientific works on this topic and determine the most optimal ways to eliminate existing shortcomings in this sphere.

Materials and Methods

The study of information security issues of the Ukrainian Defense Forces was conducted using formal logical, comparative legal and systemic-structural methods. Thus, the formal logical method was used to investigate the legal framework of information security of the defense forces of Ukraine. A comparison of the legal rules of national legislation, as well as the experience of ensuring information security of the defense forces of Lithuania and Ukraine, was carried out using the comparative legal method. The systemic-structural method allowed analyzing the latest scientific publications devoted to the study of information security issues of the state defense forces, summarize and present the results of the study.

The study of information security issues of the Ukrainian Defense Forces was conducted using general and special scientific methods: logical and sematic method, logical and legal method, method of critical analysis, comparative and legal method, systemic and structural method. The logical and sematic method made it possible to disclose the content of information, information security of the state and international information security, to reveal the difference between information security and cybersecurity, to identify subjects of the Ukrainian defense forces. The logical and legal

method was used to investigate the legal framework of information security of the defense forces of Ukraine. Method of critical analysis became the basis for analyzing the latest scientific publications devoted to the study of information security issues of the state defense forces and powers of subjects of the Ukrainian defense forces in the sphere of information security management. A comparison of the legal rules of national legislation, as well as the experience of ensuring information security of the defense forces of Lithuania and Ukraine, was carried out using the comparative and legal method. The comparative and legal method also allowed to reveal features of public-private cooperation in Germany at the sphere of information security of defense forces. The systemic and structural method was used for generalization and presentation results of the study.

Results

The legislation of Ukraine pays considerable attention to the legal regulation of the security of the information space of the state. First, the 1992 Law of Ukraine on Information enshrines the concept of "information" and its types. Second, the content of the concept of "information security" is defined at the legislative level. According to the Law of Ukraine On the Fundamental Principles of Information Society Development in Ukraine for 2007-2015 dated January 9, 2007, information security is a state of protection of vital interests of the individual, society and the state, which prevents damage caused by incomplete, untimely and unreliable information used; negative informational impact; negative consequences of the use of information technology; unauthorized distribution, use, violation of the integrity, confidentiality, and accessibility of information (Law of Ukraine…, 2007).

Third, national legislation contains definitions of information security and cybersecurity, as evidenced by the Law of Ukraine on Basic Principles of Ensuring Cybersecurity of Ukraine dated October 5, 2017, the Cybersecurity Strategy of Ukraine dated March 15, 2016, the Concept for the Development of the Security and Defense Sector of Ukraine dated March 14, 2016. At the same time, according to P.M. Snitsarenko, Yu.O. Sarycheva and V.A. Tkachenko, it is not functionally possible to separate information and

cybernetic spaces, and if we pay attention to the practical implementation of legal provisions, then the separate existence of information and cybersecurity is an unacceptable methodological mistake that negates all attempts to counteract modern information threats (Snitsarenko et al., 2018).

Fourth, in addition to legislatively defining the concept of "information security", the Doctrine of Information Security of Ukraine has identified current threats to national security in the information sphere, which include:

1. special information operations aimed at undermining defense capabilities, demoralizing personnel of the Armed Forces of Ukraine and other military formations, exacerbating and destabilizing the socio-political and socio-economic situation, stirring up interethnic and interfaith conflicts in Ukraine;

2. special information operations in other countries by the aggressor state in order to create a negative image of Ukraine in the world;

3. information expansion of the aggressor state through expansion of its own information infrastructure on the territory of Ukraine and in other states;

4. information domination of the aggressor state in the temporarily occupied territories;

5. insufficient development of the national information infrastructure, which limits the ability of Ukraine to effectively counteract information aggression, proactively act in the information sphere to realize the national interests of Ukraine;

6. inefficient state information policy, imperfect legal regulation of public relations in the information sphere;

7. insufficient level of media culture of society;

8. spreading calls for radical action, promoting autonomous concepts of coexistence of regions in Ukraine (Presidential Decree No. 47/2017…, 2017).

Analyzing the threats to the information space enshrined in the Information Security Doctrine dated February 25, 2017, it is possible to see that they are directly or indirectly aimed at destabilizing the state's capabilities in the sphere of defense, military sphere, and maximizing the blocking of capabilities of the Armed Forces of

Ukraine. Considering this, the Ministry of Defense of Ukraine introduced the military standard VST 01.004.004–2014 (01) “Information security of the state in the military sphere. Terms and definitions.” This standard is important because it defines narrower categories, thus defining “information support (in the military sphere)” as a set of measures of military authorities of all levels, actions of troops (forces) and other entities of information activities for the purpose of creating (forming) and using the necessary information resources in the information space of the military sphere for the implementation of management processes in the interests of the defense of the state (Military standard…, 2019).

O.V. Ustymenko and Yu.V. Sarychev draw attention to the fact that the specified standard leaves aside the information support of the management of the defense forces, whereas in the conditions of armed conflict in the east of Ukraine it is incumbent upon it to respond promptly to new circumstances and make informed decisions, predict its possible consequences. However, such tasks cannot be accomplished without objective information on the state of affairs in eastern Ukraine in the military and other fields. For this reason, scientists propose to optimize the definition of information support (in the military sphere) and to define in the specified standard the concept of “information support for the system of strategic management of the defense forces” as a set of measures of military management bodies of all levels and actions of troops (forces) and other subjects of information activity for the purpose of creation (formation), use and protection of the necessary information resources in the information space of military sphere and their timely provision for management processes (functions) in the interests of strategic management of the defense forces (Ustymenko and Sarychev, 2019).

At the same time, certain principles of information security of the Ukrainian Defense Forces are contained in such documents as the Military Doctrine of Ukraine of September 24, 2015 and the Strategic Defense Bulletin of Ukraine of May 20, 2016. In particular, item 17 of the Military Doctrine of Ukraine states that, based on the principles of state policy in the foreign and domestic spheres, as well as actual threats to the national security of Ukraine, one of the objectives of military

policy in the medium term is to create a unified system of intelligence and appropriate infrastructure information processing in the time mode close to real (Decree of the President of Ukraine…, 2015). This provision indicates that today Ukraine is not able to respond promptly to changes in the information space, to quickly process the necessary information for military security, which is undoubtedly a significant drawback that reduces the capabilities of the country's defense forces.

However, if we analyze the powers of the subjects of the Ukrainian defense forces, which include the Armed Forces of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the State Special Transport Service, and other military units formed in accordance with the laws of Ukraine, as well as law enforcement and intelligence agencies, in terms of involving them in the accomplishment of the state defense tasks, it can be concluded that the main part of the powers in the information sphere rests with the Foreign Intelligence Service of Ukraine and the State Special Liaison and Information Protection Service of Ukraine. The tasks of the first service are to obtain intelligence information, carry out special measures aimed at counteracting external threats to the national security of Ukraine in the information sphere, and the task of the second service is to ensure the functioning of the government communication of the Commander-in-Chief of the Armed Forces of Ukraine with officials of the Armed Forces of Ukraine, military formations, special-purpose law enforcement agencies during their stay in the control points and to ensure the cyber defense of critical infrastructure (Decree of the President of Ukraine…, 2015).

According to the Strategic Defense Bulletin of Ukraine, in order to achieve one of the operational goals of the defense reform, which should be completed by the end of 2020, it is envisaged to establish a unit for cyber defense in the structure of the Ministry of Defense of Ukraine and to implement information protection measures in accordance with the requirements of regulatory acts of Ukraine, taking into account NATO and ISO/IEC standards (Presidential Decree On the Decision…, 2016b).

Analyzing the system of authorities responsible for ensuring the information space security in Ukraine, it

is possible to make a clear conclusion about its complexity. Today, the Ministry of Defense of Ukraine, the State Service for Special Communication and Information Protection of Ukraine, the Foreign Intelligence Service of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the Office of Intelligence of the State Border Guard Service of Ukraine function in this area. In fact, it is more urgent to ensure the coordination of the activities of these entities rather than to create new ones. Another way of optimizing the activities of these entities may be to simplify their powers to protect the information space in Ukraine.

If we pay attention to the experience of Lithuania, Infostruktūra, which owns the state data transmission network, was subordinated to the Ministry of Defense of Lithuania in 2017 in order to strengthen the protection of the information space; the National Cybersecurity Center under the Ministry became the only state body in the country's defense system, which tasks include ensuring monitoring, control over the implementation of the necessary security requirements and the management of cyber incidents. The National Cyber Security Center of Lithuania monitors state information resources, analyzes the situation in the cybersecurity field, develops cybersecurity plans for critical infrastructure. The Ministry of Defense of Lithuania has the Department of Cybersecurity and Information Technology, which is responsible for shaping national policies in the field of communications and information systems and cyber defense.

It is worth paying attention to the experience of Latvia, where the Ministry of Defense combined the functions of the state's cybersecurity and electronic security services. In particular, in 2013, the Ministry of Defense took over the management of the National Council for Information Technology Security. In addition, in 2014, the cybersecurity unit, Emerson Security, was formed within the structure of the National Armed Forces of the Republic of Latvia. A feature of its activity is the involvement of private and public sector representatives simultaneously in order to prevent cyber-incidents and minimize the effects of cyber-incidents (Hapieieva, 2017). To strengthen the security of the information space of the Ukrainian Defense Forces, it is important to update

the relevant system of subjects and to improve the interaction between them, to establish public-private cooperation, to provide qualified personnel, etc.

Discussion

Improving the information security of the Ukrainian Defense Forces is an issue that requires a comprehensive approach; one of the possible areas is updating the system of entities responsible for collecting, storing and protecting strategic information of the state defense forces. At the same time, interaction should be established between these entities. In support of the above, we note that, according to S. Boes and E.R. Leukfeldt, a formalized cooperation between public authorities and stakeholders is one of the ways to strengthen the information security of the state (Boes and Leukfeldt, 2017). In the field of public-private cooperation, the experience of Germany is progressive, where the Law on Information Security was adopted to prevent attacks on important information systems of the state. It enshrines the basic principles of interaction between the state, which is represented by the relevant authorities, and citizens. This law sets minimum information security standards for critical infrastructure companies. Accordingly, these minimum requirements must be ensured through the accessibility, authenticity, confidentiality and integrity of IT security throughout Germany, enhancing Internet security for citizens, introducing uniform standards for the protection of national critical infrastructure (Boiko, 2018).

For Ukraine, the experience of these states is new, but it can be used to improve the state of information security of the defense forces in the country). Obviously, in Germany, the basis for public-private cooperation in the field of protecting the information space is the establishment of uniform requirements, which simplifies the monitoring of compliance by entities with these requirements and improves communication between the state and citizens. Considering the improvement of information security of the defense forces in Ukraine, it would be advisable to use the experience of Germany and legislatively introduce uniform standards of information security for defense forces and critical infrastructure.

Particular attention should be paid to staffing the defense forces with qualified personnel in the field of

protecting the information space. Without a detailed description of the personnel of each structure belonging to the defense forces, we suggest focusing on the personnel policy of the Armed Forces of Ukraine. In particular, the analysis of the content of the Concept of Military Personnel Policy in the Armed Forces of Ukraine until 2020 (Concept of military…, 2020) leads to the conclusion that there is no emphasis on the need to provide them with experts in the information security and cybersecurity, although there is an indication that the need to improve military personnel policy is driven by changes in national policy priorities in the national security and defense sector, reforms envisaged by the Association Agreement between Ukraine and the European Union, ratified by Law of Ukraine No. 1678-VII dated 16 September 2014 and the need to enhance the interoperability of the Armed Forces of Ukraine with NATO member states' armed forces to complete common missions and training. Thus, it is advisable to pay attention to this in the above concept and to make efforts in this direction.

Conclusion

Thus, it is almost impossible to determine one area in terms of improving the security of the information resources of the defense forces, given their interrelation; accordingly, the development of one of these areas should take into account all aspects. The legislation of Ukraine defines the concepts of "information", "information security", and "defense forces". The legislator distinguishes between "information security" and "cybersecurity", which significantly complicates the legal regulation of the protection of the information space of the state and is not supported by some scientists. It is emphasized that the optimization of the information security of the state as a whole and the defense forces of Ukraine requires optimizing the system of entities responsible for protecting the information space, creating conditions for public-private cooperation in this area, following the example of Germany, and providing these entities with qualified employees.

References:

Boes S, Leukfeldt ER. (2017). Fighting cybercrime: a joint effort. Cyber-Physical Security: Protecting Critical

Infrastructure at the State and Local Level, 3, 185-203.

Bohdanovych VYu, Vorovych BO, Marko YeI. (2018). Information security as a basis for military security of the state and society. Collection of Scientific Works of the Center for Military and Strategic Studies of Ivan Chernyakhovsky National University of Defense of Ukraine, 3, 44-48.

Boiko VO. (2018). Public-private Partnership in Cybersecurity? Kyiv: National Institute for Strategic Studies, 18.

Concept of military personnel policy in the Armed Forces of Ukraine until 2020. (2020). http://www.mil.gov.ua/diyalnist/kadrova-politika/konczepcziya-kadrovoi-politiki-v-zbrojnih-silah-ukraini/.

Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine as of September 2, 2015 on the new version of the Military Doctrine of Ukraine as of September 24, 2015. (2015). https://zakon.rada.gov.ua/laws/show/555/2015.

Hapieieva O. (2017). Cyber security in the Baltic States: a historical retrospective. SKhID, 6(152). DOI: 10.21847/1728-9343.2017.6(152).120038. http://skhid.kubg.edu.ua/article/view/120038.

Kosohov OM. (2016). Information security in the sphere of defense as a component of Ukraine's military security. Information Processing Systems, 8(145), 115-117.

Law of Ukraine on the Fundamental Principles of Information Society Development in Ukraine for 2007-2015 as of January 09, 2007. (2007). https://zakon.rada.gov.ua/laws/show/537-16.

Military standard. Information security of the state in the military sphere. Terms and definitions: VST 01.004.004 – 2019 (02). (2019). Kyiv: Ministry of Defense of Ukraine. https://nuou.org.ua/assets/documents/VST_%2001-004-002_2019.pdf.

Nieles M, Dempsey K, Pillitteri VYa. (2017). An introduction to information

security. NIST Special Publication. DOI: 10.6028/NIST.SP.800-12r1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

Pelevina ES. (2017) Political problems of international relations, global and regional development. Theories and Problems of Political Studies, 6(1A), 194-205.

Presidential Decree No. 47/2017 on the Decision of the National Security and Defense Council of Ukraine as of December 29, 2016 on the Doctrine of Information Security of Ukraine as of February 25, 2017. (2017). https://www.president.gov.ua/documents/472017-21374.

Presidential Decree on the Decision of the National Security and Defense Council of Ukraine as of March 4, 2016 on the Concept of Development of the Security and Defense Sector of Ukraine as of March 14, 2016. (2016a). https://zakon.rada.gov.ua/laws/show/92/2016#n12.

Presidential Decree on the Decision of the National Security and Defense Council of Ukraine of May 20, 2016 on the Strategic Defense Bulletin of Ukraine as of June 06, 2016. (2016b). https://zakon.rada.gov.ua/laws/show/240/2016#n10.

Reznik O, Getmanets O, Kovalchuk A, Nastyuk V, Andriichenko N. (2020). Financial security of the state. Journal of Security and Sustainability Issues, 9(3), 843-852. DOI: 10.9770/jssi.2020.9.3(10).

Seng AHW. (2016). Cyber attacks and the roles the military can play to support the national cyber security efforts. Pointer, 42(3), 27-37.

Snitsarenko PM, Sarycheva YuO, Tkachenko VA. (2018). General theoretical prerequisites for the need to improve the current legislation of Ukraine on information security of the state. Collection of Scientific Works of the Center for Military and Strategic Studies of Ivan Chernyakhovsky National University of Defense of Ukraine, 1, 62-67.

Transforming our World: The 2030 Agenda for Sustainable Development. United Nations. (2015).

https://sustainabledevelopment.un.org/post2015/transformingourworld.

Ustymenko OV, Sarychev YuO. (2019). Information support for the system of strategic management of the defense forces. Bulletin of the National Academy of Public Administration under the President of Ukraine. Series State Management, 1, 11-17.

Vakulyk OO, Andriichenko NS, Reznik OM, Volik VV, Yanishevska KD. (2019). International aspect of a legal regulation in the field of financial crime counteraction by the example of special services of Ukraine and the CIS countries. Journal of Legal, Ethical and Regulatory Issues, 22(1). https://www.abacademies.org/articles/International-aspect-of-a-legal-regulation-in-the-field-of-financial-crime-counteraction-by-the-example-of-special-services-of-Ukraine-and-the-CIS-countries-1544-0044-22-1-280.pdf