JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 March Volume 9 Number 3
https://doi.org/10.9770/jssi.2020.9.3(4)

CYBERSECURITY AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE

Olga Vakulyk[1], Pavlo Petrenko[2], Iulia Kuzmenko[3], Maksym Pochtovyi[4], Ruslan Orlovskyi[5]

[1]National Academy of Internal Affairs, Solomensky Square, 1, Kyiv, 02000, Ukraine*
[2]ex-Minister of Justice, 13 Gorodetskogo str., Kyiv, 01001, Ukraine
[3]Kherson Faculty Odesa State University of Internal Affairs, st. Fonvizina, 1, Kherson, Ukraine
[4]Kryvyi Rig Faculty of Dnipropetrovsk State University of Internal Affairs, 7th Zarechny district, 24, Kryvyi Rih, 50000, Ukraine
[5]Yaroslav Mudryi National Law University, 77 Pushkinskaya st., Kharkiv, 61024, Ukraine

E-mail: [1]koaduep@gmail.com*

Received 23 March 2019; accepted 20 December 2019; published 30 March 2020

Abstract. The article is devoted to the study of cybersecurity as a component of the national security of the state. It has been established that the development of information and telecommunication technologies testifies to the progress of society but also determines the security risks of their use. In particular, this refers to a cyberattack and other cyberthreats. It has been determined that cybersecurity should be understood as the protection of the vital interests of a person and citizen, society and the state when using cyberspace. An important role in ensuring such a security is played by the cyberthreat protection mechanism, which provides for the development and adoption of a cybersecurity strategy, the creation of a national cybersecurity system, strengthening of the security and defense sector's capabilities to effectively combat military cyberthreats, cyberterrorism, and ensuring cyberprotection of state electronic information resources and information infrastructure. The existence of the Cybersecurity Strategy of Ukraine and other acts as the legal basis for countering cyberthreats has been noted. In turn, the national cybersecurity system provides for the activities of the Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the National Bank of Ukraine, and intelligence agencies. In turn, in France, Finland, Germany, the central place in the cybersecurity system belongs to the National Cybersecurity Agency, the National Cybersecurity Center, and the Cyberdefense Center, respectively. Despite Ukraine's significant steps towards increasing cybersecurity in the state, there is no public-private cooperation in this area. Due to this, authorized entities should establish cooperation with the non-state sector and establish effective institutional and legal instruments for such cooperation. At the same time, the issue of public-private cooperation in the field of cybersecurity is relevant for all states of the world in view of the global nature of existing cyberthreats.

Keywords: national security; cybersecurity; cyberdefense; cyberthreats; cyberattack; information; information infrastructure

Reference to this paper should be made as follows: Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., Orlovskyi, R. 2020. Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues,* 9(3), 775-784. https://doi.org/10.9770/jssi.2020.9.3(4)

JEL Classifications: F35; F42

1. Introduction

The development of information and telecommunication technologies leads to a number of security risks for their use. So, more than half of the world's population uses the Internet. By the end of 2018, 51.2% of the world's population, which is equivalent to 3.9 billion people, uses the Internet. This is an important step towards a more global information society, but it also demonstrates the need for enhanced cyberdefense. According to data provided by ITU Connect, by 2023, 70% of the global population will be free to use the Internet, which once again demonstrates the need for more cybersecurity.

At the same time, the significant threats to the safe use of the Internet for searching, storing, and disseminating information, conducting banking transactions and other transactions, software of work of enterprises, institutions, organizations are cyberthreats, including cyber-attacks. In particular, not so long ago, Ukraine faced another cyberattack, possibly the most serious in its history. The virus designated as «Petya», «Petya.A», «PetrWrap», «GoldenEye», «Diskcoder.C» quickly spread among Ukrainian systems, temporarily disabling government agencies, airports, banks, media companies, delivery services, and even radiation monitoring systems at the former Chernobyl nuclear power plant. At the same time, the damage was caused to a number of companies in the USA, the Russian Federation, Great Britain, France, and Australia (Nekrasov V., Polyakova A., 2017). Such a situation testifies, firstly, to the current dependence of a number of processes on computer technologies, and, secondly, to their insecurity in Ukraine from cyberattacks. This is confirmed by the fact that, according to official data, the National Cybersecurity Index in the state as of 2018 is 58.44%. That is, Ukraine is only 50% ready to prevent fundamental cyberthreats and combat cybercrime, develop a national cyberdefense policy, and provide electronic identification and signature services (National CyberSecurity Index, 2018).

The study of the issue of cybersecurity as a component of the national security of the state is no a coincidence, since today the cyberattack designated as Petya, Petya.A, PetrWrap, GoldenEye, Diskcoder.C have clearly demonstrated the existing gaps in ensuring cybersecurity not only in Ukraine but also in other countries of the world. So, due to the globalization of cyberspace, all states without exception are interested in safe cyberspace.

2. Literature Survey

Zine Homburger points out that the cybersecurity capacity development is a way to empower people, communities and governments' capabilities to achieve their development goals by reducing the digital security risks associated with accessing and using information and communication technologies. This definition emphasizes not only the development of the state's potential to achieve the desired level of cybersecurity but also minimizes the negative consequences of the use of information and computer technologies (Homburger, 2019).

However, despite the fact that the perception of cybersecurity as one of the priority areas of national security is widespread among both developed and transitional states in the modern globalized world, today there is no single definition of the term «cybersecurity» in scientific doctrine (Drobyazko et. al., 2019a, 2019b). Thus, G.V. Foros and K.S. Kondrasheva note that cybersecurity is the security of information and information infrastructure in the digital environment, and information security allows achieving such goals as confidentiality of information; the integrity of information and related processes; availability of information; monitoring of all such processes" (Foros G.V., Kondrasheva K.S., 2016). In turn, Miguel Ferreira Da Silva notes that in France cybersecurity is considered as the desirable state of information systems, in which they may be confronted with external factors that could threaten the availability, integrity or confidentiality of stored, processed or transmitted data, as well as the related services the systems provide (Da Silva, 2016).

Rossouw von Solms and Johan van Niekerk focus on the fact that cybersecurity is the protection of cyberspace, electronic information, information and computer technologies that support cyberspace, as well as a person as a user of cyberspace. The given understanding of the concept of "cybersecurity" automatically separates it from the essence of another similar definition "information security". According to scientists, vivid examples of existing threats that relate exclusively to cybersecurity, and not information security, include: (a) cyberbullying, which has become a major issue in modern society, as modern technology is increasingly used for bullying, provoking violence and causing psychological harm; (b) smart home that became possible due to the emergence of new technologies that allow controlling the home on a remote basis, which is convenient enough, at the same time this advantage is posed by a significant threat that an unauthorized person will gain unauthorized access to the home by breaking the security system of the technologies use (Sitdikova & Starodumova, 2019); (c) digital media, according to the data, it is the entertainment industry that announces more losses annually because of the possibility of unauthorized distribution of films, songs, gaming applications, directly damages the copyright holders; (d) cyberterrorism, most often encroaching on critical infrastructure objects, protection of which is an important component of cybersecurity policy (Rossouw von Solms, Johan van Niekerk, 2013). All this indicates that cybersecurity covers a wider range of issues than information security. In turn, information security, for example, may consist of unlawful access, disclosure, and destruction of information that is recognized as bank secrecy, which occurs among employees of banks and banking institutions (Klochko, A.N., Kulish, A.N., Reznik, O.N., 2016).

Complementing the rather comprehensive classification proposed by scientists, Sharikov Pavel A. emphasizes at least three elements that each, without exception, cyberthreat contains: (1) sources; (2) goals and (3) means of implementation of cyberattacks. In doing so, all components of cyberthreats must be taken into account when developing a robust cybersecurity strategy (Sharikov, Pavel A., 2019).

In order to create the necessary conditions for the safe functioning of cyberspace and for its use in the interests of the individual, society, and the state, it is necessary not only to develop a cybersecurity strategy but also as it is emphasized by Tomas Plėta, Sergii Karasov, Tadas Jakštas: (a) to create a national cybersecurity system which N. Tkachuk considers as the totality of all entities ensuring state cybersecurity, the mechanism of their interaction and coordination, a set of measures to protect against cyberthreats, counter cyberterrorism, and cyberintelligence, as well as the legal framework governing the field of cybersecurity (N. Tkachuk, 2018); (b) to strengthen the capabilities of the security and defense sectors to ensure the effective fight against military cyberthreats, cyberespionage, cyberterrorism and cybercrime, and to deepen international cooperation in this field; (c) to ensure cyberprotection of state electronic information resources, necessary information, as well as information infrastructure.

3. Methods

Ensuring the cybersecurity of the state is a complex process, in which more than one authorized entity must participate using more than one method. Among such methods, it is necessary to single out, first of all, the legal method, which allows correctly determining the theoretical foundations of protecting cyberspace and creating a legal framework for the activities of entities of the national cyberdefense system. The activities of the relevant public and private entities are the result of the use of the organizational method, which allows, based solely on the current state of cyberspace of the state, determining the need for new entities, creating them and providing all conditions for their effective functioning. One should not forget about technological methods because without software and technologies it will be impossible to counteract cyberthreats.

Thus, the protection of the state's cyberspace is a systematic activity of the state, which is based on such legal, organizational, and technological methods.

4. Results

The Law of Ukraine «On Basic Principles of Ensuring Cybersecurity of Ukraine» dated 5 October 2017 defines cybersecurity as the protection of the vital interests of a person and citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely identification, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace. In turn, the legislator of Ukraine relates the following points to the cybersecurity objects: (1) constitutional rights and freedoms of man and citizen; (2) society, sustainable development of the information society and digital communication environment; (3) the state, its constitutional system, sovereignty, territorial integrity, and inviolability; (4) national interests in all spheres of life of an individual, society and state; (5) critical infrastructure facilities (Law on the Fundamentals of Cybersecurity of Ukraine, 2017).

Thus, article 17 of the Constitution of Ukraine stipulated that protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian nation (Constitution of Ukraine, 1996). At the same time, although cybersecurity is not explicitly mentioned in this constitutional norm, even though only the most important areas of protection are taken into account, it can be concluded that cybersecurity is an integral part of information security.

The Law of Ukraine «On Information» provides that the main directions of state policy in the information sphere include, in particular: (a) assurance of access to information for everyone; (b) ensuring equal opportunities regarding the creation, collection, receipt, storage, use, distribution, security, protection of information; (c) creation of conditions for the formation of an information society in Ukraine; (d) assurance of the openness and transparency of the activities of entities of power; (e) creation of information systems and information networks, the development of electronic management; (f) continuous updating, enrichment, and storage of national information resources; (g) assurance of information security of Ukraine; (h) the promotion of international cooperation in the information sphere and the entry of Ukraine into the global information space. However, it is obvious that, in this normative legal act, the legislator focuses exclusively on the concept of "information security" (Law of Ukraine on Information, 1992). Therefore, it is advisable to pay attention to other normative legal acts and provisions of the scientific doctrine, which pay attention to the existing cyberspace threats, as well as a list of measures that should be implemented to minimize them.

In particular, the National Security Strategy of Ukraine approved by the Decree of the President of Ukraine «On the decision of the National Security and Defense Council of Ukraine dated 6 May 2015, «On the National Security Strategy of Ukraine» dated 26 May 2015, identifies among the main threats to cybersecurity and the security of information resources: (1) vulnerability of critical infrastructure facilities, state information resources in cyberattacks, (2) the physical and moral obsolescence of the state secret protection system and other types of information with the restricted information (National Security Strategy of Ukraine, 2015).

Mykola Syomych, Iryna Markina, Dmytro Diachkov highlight, in accordance with the National Cybersecurity Index, the following cyberprotection weaknesses in Ukraine: (a) lack of protection of digital services (lack of responsibility of providers for digital services), cybersecurity standards for the public sector and the competent cybersecurity oversight body) (b) lack of cybercrisis management practices at the national level, indifference to international activities in the field of cybercrisis management, lack of operational support for volunteers during the cybercrisis; (c) lack of military cyberoperations (lack of units to implement military cyberoperations, indifference to international initiatives, lack of experience in conducting military cyberoperations) (Mykola Syomych, Iryna Markina, Dmytro Diachkov, 2018).

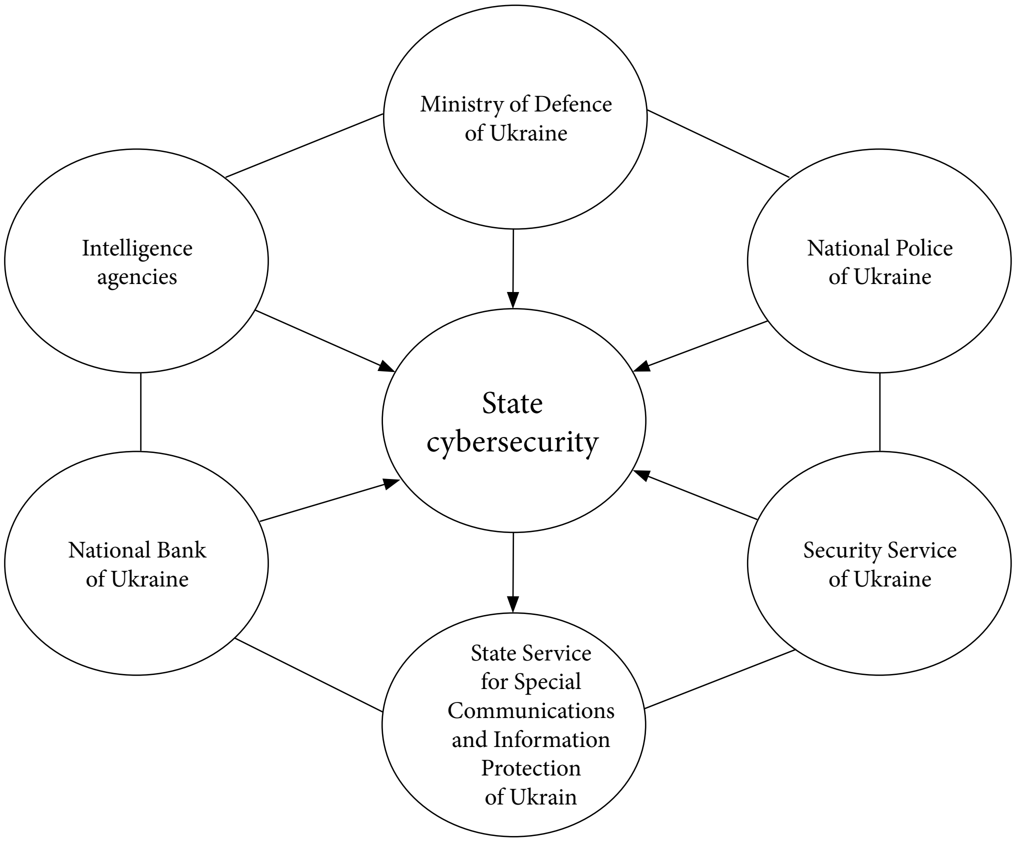
Ministry of Defence of Ukraine
Intelligence agencies
National Police of Ukraine
State cybersecurity
National Bank of Ukraine
Security Service of Ukraine
State Service for Special Communications and Information Protection of Ukrain

Figure 1. System of entities of the national cybersecurity system of the country according to the Cybersecurity Strategy of Ukraine 2016

Although the main directions of achieving the necessary operational and other capabilities of the components of the country's security and defense sector as a whole have been emphasized in the decision of the Council of National Security and Defense of Ukraine dated 4 March 2016 «On the Concept for the Development of the Security and Defense Sector of Ukraine», it is worth highlighting among them also those related specifically to cybersecurity, in particular: improving public administration and management of the security and defense sector, including: (a) information and cybersecurity systems; (b) information protection and information resource security systems; (c) intensification of the fight against military cyberthreats; (d) cyberespionage; (e) cyberterrorism; (f) cybercrime; (g) deepening international cooperation in this area (Concept for the development of the security and defense sector of Ukraine, 2016).

In addition to the general National Security Strategy of Ukraine, the Cybersecurity Strategy of Ukraine was also approved, which in particular defines the entities of the state's national cybersecurity system (Figure 1).

Thus, the Ministry of Defense of Ukraine, in accordance with the provision approved by the resolution of the Cabinet of Ministers of Ukraine dated 26 November 2014, is the main body in the system of central executive bodies, which ensures the formation and implementation of state policy regarding the national security in the military sphere, the defense and military construction spheres during peacetime and special period. It is worth noting that only in 2019 its competence was supplemented with powers to take measures to ensure information security, cybersecurity, and cyberdefense, as well as prepare the state to repel military aggression in cyberspace (cyberdefense) (Regulation on the Ministry of Defense of Ukraine, 2014).

The structure of the Ministry of Defense of Ukraine provides for the activities of the Office of Information Technology, the purpose of which is to ensure, during peacetime and a special period, the implementation of the state policy regarding the information security, cybersecurity, and informatization in the system of the ministry, to organize and coordinate measures for the implementation of the latest information technologies, the formation of a single information infrastructure of the ministry. At the same time, the Office of Information Technologies of the Ministry of Defense of Ukraine is also involved in monitoring the information environment, identifying potential and real information and cyberthreats to the national security of Ukraine in the field of defense and assessing the level of military threat to the national security of Ukraine, conducting information and analytical activities and forecasting the development of events related to the implementation of potential and real information and cyberthreats.

The next entity of the national cybersecurity system is the State Service for Special Communications and Information Protection of Ukraine, which works today exclusively with cybersecurity issues. The main activities of the service include interaction with the UA administrative domain; protection of state information resources; interaction with public authorities and international cooperation in the field of protection of information resources; assurance of the functioning of a unified anti-virus protection system; determination of the level of protection of information systems and telecommunications.

N. Tkachuk emphasizes that the state's cybersecurity system should be developed in accordance with existing cyberthreats, which it must counter. According to the scientist, the greatest danger to the state today is the unlawful cybernetic influence of special services of foreign states and terrorist organizations on the critical infrastructure of the state. Therefore, special attention should be paid to the status of the Security Service of Ukraine as a special-purpose law enforcement agency and its competence to prevent external and internal threats to state security, intelligence, terrorism and other illegal attacks by special services of foreign states, organizations, individual groups, and individuals on the vital interests of Ukraine, and also counteracting special information operations against Ukraine in cyberspace. The status of special services indicates its key role in the National Cybersecurity System of Ukraine, which is to provide counterintelligence protection of state interests in the field of cybersecurity through: (1) countering cyberespionage and cyberterrorism; (2) the detection and disclosure of cybercrime (Tkachuk, 2017; Korauš, et. al., 2019).

Along with the Security Service of Ukraine, another law enforcement agency operates - the National Police of

Ukraine as an entity of the National Cybersecurity System of Ukraine. In the structure of the police bodies, the Cyberpolice Department of the National Police of Ukraine was created. At the same time, Bereza V. suggests under the authority of the Cyberpolice Department of the National Police of Ukraine to consider the established system of legal rights (measures of possible behavior) and legal duties (measures of necessary behavior) that the Cyberpolice Department of Ukraine has in order to exercise law enforcement functions (Bereza, V. 2018). And according to information on the official website of the said body, its tasks include: (a) implementation of state policy in the field of combating cybercrime; (b) timely informing the population about the emergence of new cybercriminals; (c) the introduction of software to systematize cyberincidents; (d) responding to requests from foreign partners.

So, in 2018, the Cyberpolice Department of Ukraine conducted an investigation of criminal offenses in the field of cybersecurity - 2688, in the field of illegal content - 1139, in the field of electronic commerce – 3607, and in the field of payment systems - 3697 (Ostrovoy A.V., 2018).

With that, the practice of the activities of the relevant cyberunits in the structure of the police is not new to foreign countries. In particular, the Cybercrime Department was created in the structure of the Central Criminal Police Directorate of the Ministry of Internal Affairs of Georgia in December 2012 by the Decree of the Minister of Internal Affairs. Currently, the department has 15 investigative detectives investigating cybercrime offenses, as well as providing advice and other assistance in investigating cybercrime and handling electronic evidence by the police units throughout Georgia.

It is worth noting that the powers of the National Police of Ukraine and the Security Service of Ukraine as entities of a cybersecurity system are similar, however, the distribution of their functions is related to the sphere of responsibility of the police and special services. Thus, the National Police bodies give key attention to protecting the rights of people, companies, institutions, organizations, and the interests of the state and society against illegal actions. In turn, the activities of the Security Service of Ukraine focus on protecting only the state, its constitutional order, state security, as well as conducting counter-intelligence activities.

Taking into account such powers of the police and special services of Ukraine in the field of cyberspace protection, an important role belongs to the interaction between these entities, which A. I. Bespalova conditionally divides into internal (within the framework of police bodies and units) and external. Depending on the directions of their activity, the scientist proposes to distinguish the following types of interaction between these entities: (1) interaction regarding the counteraction to the offenses in the field of telecommunications; (2) interaction regarding the counteraction to the offenses in the field of electronic commerce; (3) interaction regarding the counteraction to the offenses in the field of fraud and legalization (laundering) of proceeds of crime, etc. (Bezpalova O.I., 2017).

As to the National Bank of Ukraine in the system of entities of the cybersecurity system of Ukraine, it is worth noting that it has limited competence in the field of ensuring cyberspace since its authority in this area relates only to cybersecurity in the activities of banks. So, according to the Law of Ukraine «On the National Bank of Ukraine» dated 20 May 1999, the National Bank of Ukraine is authorized to determine the procedure, requirements, and measures to ensure cyberprotection and information security in the banking system of Ukraine and for the entities transferring funds, to monitor their implementation, and also to create the cyberprotection center of the National Bank of Ukraine, and to ensure the functioning of the cyberprotection system in the banking system of Ukraine (Law of Ukraine on the National Bank of Ukraine, 1999).

After the Petya virus blocked the work of banks, the National Bank of Ukraine adopted the Decree No. 95 “On approval of the Regulation on the organization of measures to ensure information security in the banking system of Ukraine”, which obliged banks to take measures during 2018 to strengthen their cybersecurity. In accordance with the said act, each bank must create a collective body on the implementation and operation of the information security management system («ISMS») and appoint a person responsible for information security, as well as update the information security system in accordance with international standards. Thus, banks were required to present their updated cybersecurity systems. However, this act of the National Bank of Ukraine did not provide for special sanctions for violation of established requirements (Pavlovska, A., Khalimon, Z., 2018).

It is worth noting that in France, the National Cybersecurity Agency (ANSSI), whose activities are controlled by the Prime Minister, belongs to the cybersecurity and cyberdefense authorities. ANSSI recognizes that the French economy cannot develop without modern technologies and therefore directs its activities to promote safe cyberspace while maintaining user privacy in order to preserve a competitive state economy (Robert S. Dewar, 2018).

In Finland, the National Cybersecurity Center (NCSC-FI) was established in 2014 as a national body for information security, which supports government agencies, the business community, and other entities in supporting cybersecurity. The center was created by combining the functions of CERT-FI and GOV-CERT with the National Communications Security Authority FICORA (NCSA-FI). Today, the National Cybersecurity Center of Finland: (1) provides information on the real state of cybersecurity in the state; (2) detects and analyzes existing cyberthreats; (3) provides available resources and means to support authorities; (4) establishes cooperation regarding the cyberspace security issues at the national, interstate, and international levels. The Centre’s responsibilities also include responsibility for the security of the transmission and processing of classified information by electronic means (Robert S. Dewar, 2018).

The Cyberdefense Center (Cyber-AZ) also operates in Germany, which is subordinate to the Federal Office for Information Security (BSI). Within its competence, Cyber-AZ collaborates with the Federal Office for Civil Protection and Disaster Management and the Federal Office for Protection of Constitution. In addition, the activities of Cyber-AZ are comprehensively supported by the Federal Criminal Police Directorate, the Federal Police Directorate, the Federal Intelligence Service, and the military bodies. Thanks to such an extensive network of entities and cooperation between them, Cyber-AZ is an important center for the exchange of information and best practice. Accordingly, Cyber-AZ evaluates cyberattacks, identifies channels for their implementation, persons who are responsible for their perpetration, and provides relevant information with recommendations to the National Cybersecurity Council (Robert S. Dewar, 2018).

5. Discussion

In their opinion of Boes, S., Leukfeldt, E.R. the law enforcement agencies play an important role in the fight against cybercrime and it is difficult to disagree with this. However, one of the strategies to combat this type of crime is to form partnerships with private institutions themselves - formalized cooperation between government bodies and stakeholders (Boes, S., Leukfeldt, E.R., 2017).

In particular, Streltsov, Lev notes that the system of entities that have the task of ensuring the cybersecurity of Ukraine can be divided into four main groups: defense and (counter) intelligence structures, law enforcement agencies, technical protection regulators, private sector, and coordinator - the National Cybersecurity Coordination Center. Moreover, the higher the level of threat to the cybersecurity of the state, the higher the likelihood that various entities should work together. Although during the latest incident related to the spread of the Petya virus, various structures were cooperating, the meaning of such cooperation is not freely accessible to the public, and therefore it cannot be evaluated by them. Another important point is the role of the private sector in ensuring cybersecurity. In Ukraine, the sphere of public-private partnerships is only at an early stage of its foundation: the legal framework for such a cooperation is not fully developed. In addition, Ukraine still lacks specialized research institutions that can contribute to cybersecurity. At the same time, it is worth noting that these problems are not significant only for Ukraine, the issue of the functioning of public-private partnerships is discussed even in states that have an improved legal system (Streltsov, Lev, 2017).

D. Dubov, V. Boiko, S. Hnatyuk, T. Isakova, M. Ozhevan, A. Pokrovska also note that in Ukraine today there is no public-private cooperation in the field of cybersecurity. In the context of the unsatisfactory state of cyberspace protection, this issue is becoming increasingly important. Accordingly, the priority task of the competent authorities is to establish communication/cooperation with the non-governmental sector and effective institutional and legal tools for this type of communication/cooperation. Another problem that is relevant is the closed nature of the Ukrainian cybersecurity sector since the available information does not provide an objective picture of its status and prospects (D. Dubov, V. Boiko, S. Hnatyuk, T. Isakova, M. Ozhevan, A. Pokrovska, 2018).

At the same time, Tkachuk Nataliya draws attention not only to the problem of public-private cooperation in the field of cybersecurity but also to the fact that despite the ratification by Ukraine of the Cybercrime Convention of the Council of Europe in 2005 as an important tool of international cooperation in the fight against cybercrime, Ukraine still has an urgent need to optimize existing mechanisms for the exchange of information between entities, including a mutual legal assistance treaty to ensure a quick and adequate response to cyberthreats and investigation of cybercrimes at national and international levels (Tkachuk, Nataliya, 2018).

Conclusions

Thus, one of the significant threats to the safe use of the Internet for searching, storing, disseminating information, conducting banking transactions and other transactions, the software of enterprises, institutions, organizations is cyberthreats, including cyberattacks. Each country's cyber-security mechanism provides for the development and adoption of a cybersecurity strategy, the establishment of a national cybersecurity system, the strengthening of the security and defense capabilities to effectively combat cyberthreats, cyberterrorism, etc., the provision of cybersecurity for state electronic information resources and information infrastructure.

In Ukraine, in addition to the Cybersecurity Strategy of Ukraine, the legal basis for counteracting and combating cyberthreats consists of the Constitution of Ukraine, the Law of Ukraine «On Basic Principles of Cybersecurity of Ukraine», the Law of Ukraine «On Information», the National Security Strategy of Ukraine, the Concept of Development of the Security and Defense Sector of Ukraine, etc. In turn, the national cybersecurity system envisages the activities of such authorized entities as the Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the National Bank of Ukraine, and intelligence agencies. A special place among these entities belongs to the Cyberpolice Department of Ukraine. In turn, in France, Finland, Germany, in contrast to Ukraine, the central place in the cybersecurity system is occupied by the National Cybersecurity Agency, the National Cybersecurity Center, and the Cybersecurity Center respectively.

Despite a number of significant steps by Ukraine towards increasing the level of protection of the state's interests against cyberthreats in the country, there is no public-private cooperation in the field of cybersecurity. The primary focus of the state's activity in this direction should be establishing communication/cooperation with the non-state sector and establishing effective institutional and legal instruments for this communication/cooperation. At the same time, the issue of public-private cooperation in the field of cybersecurity is urgent for all, without exception, countries of the world, given the global nature of existing cyberthreats.

References

Bereza, V. (2018). Concept and classification of powers of the Cyberpolice Department of the National Police of Ukraine. *Bulletin of Kharkiv National University of Internal Affairs*. http://doi.org/10.32631/v.2018.3.03

Boes, S., Leukfeldt, E.R. (2017). Fighting Cybercrime: A Joint Effort. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level,* 3, 185–203.

Cybercrime and cybersecurity strategies in the Eastern Partnership region (2018). URL: https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

Da Silva, M.F. (2016). Cyber Security vs. Cyber Defense – A Portuguese View On the Distinction. URL: https://www.academia.edu/23986861/CYBER_SECURITY_VS._CYBER_DEFENSE_A_PORTUGUESE_VIEW_ON_THE_ DISTINCTION

Dewar, Robert S. ed. (2018). National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1, 2018, Center for Security Studies (CSS), ETH Zürich.

Drobyazko, S., Alieksieienko, I., Kobets, M., Kiselyova, E., Lohvynenko, M. (2019). Transnationalisation and segment security of the international labor market. *Journal of Security and Sustainability Issues* 9(2) http://doi.org/10.9770/jssi.2019.9.2(14)

Durmanov, A., Bartosova, V., Drobyazko, S., Melnyk, O., Fillipov, V. (2019). Mechanism to ensure sustainable development of enterprises in the information space. *Entrepreneurship and Sustainability Issues*, 7(2), 1377-1386. http://doi.org/10.9770/jesi.2019.7.2(40)

Dubov D., Boiko V., Hnatyuk S., Isakova T., Ozhevan M., Pokrovska A. (2018) Public-private partnership in cybersecurity: international experience and opportunities for Ukraine : analytical report; General editorship of D. Dubov. Kyiv, 84 p.

Klochko, A.N., Kulish, A.N., Reznik, O.N. (2016). The social basis of criminal law protection of banking in Ukraine. *Russian Journal Of Criminology*. http://doi.org/10.17150/2500-4255.2016.10(4).790-800

Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. (2019). Using quantitative methods to identify insecurity due to unusual business operations, *Entrepreneurship and Sustainability Issues,* 6(3), 1101-1012. . http://doi.org/10.9770/jesi.2019.6.3(3)

Kostyuk N., Geers K. (2015). Ukraine: A Cyber Safe Haven? Cyber War in Perspective: Russian Aggression against Ukraine. Pp. 113-122.

Homburger Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society*. https://doi.org/10.1080/13600826.2019.15695 02

Mykola Syomych, Iryna Markina, Dmytro Diachkov (2018). Cybercrime as a leading threat to information security in the countries with transitional economy. *Advances in Social Science, Education and Humanities Research: 2nd International Conference on Social, economic, and academic leadership,* 217., 342–350.

National Cyber Security Index (2018). URL: https://ega.ee/wp-content/uploads/2018/05/ncsi_digi tal_smaller.pdf.

Rossouw von Solms, Johan van Niekerk (2013). From information security to cyber security. *Computer and Security.* Issue 38. P. 97–103.

Nekrasov V., Polyakova A. (2017). This is war: Ukraine was shaken by the largest cyberattack in history. *Ekonomichna Pravda*. URL: http://www.epravda.com.ua/publications/2017/06/27/626518/

Ostrovoy A.V. (2018). Analysis Of the Conditions For the State Policy Formation To Ensure Kibernetic Security in Ukraine. *Public Governance* https://doi.org/10.32689/2617-2224-2019-17-2-296-306

Pavlovska, A., Khalimon, Z. (2018). Cyber security in the bank sector: can IT outsourcing help? URL: http://yur-gazeta.com/legal-business/articles-in-english/cyber-security-in-the-bank-sector-can -it-outsourcing-help.html

Sharikov, Pavel A. (2019). Evolution of American Cyber Security Policies. *Mirovaya Ekonomika i Mezhdunarodnye Otnosheniya*. http://doi.org/10.20542/0131-2227-2019-63-10-51-58

Sitdikova, L.B.; Starodumova, S.J. (2019). Corporate agreement as a means of providing security in the course of entrepreneurship development, *Entrepreneurship and Sustainability Issues,* 7(1), 324-335. http://doi.org/10.9770/jesi.2019.7.1(24)

Streltsov, Lev (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research* http://doi.org/10.1007/s41125-017-0020-x

Tkachuk, Nataliya (2018). Countering Cyber Threats to National Security: Ukraine Defends Its Cyber Infrastructure in the Face of Attacks from Russia. URL: https://www.researchgate.net/publication/328232415

Tkachuk, Nataliya (2017). The Role and Place of the Security Service of Ukraine in the National Cyber Security System. *The Journal of Eastern European Law*, 44, 50-57.

Bezpalova O.I. (2017). Interaction of the National Police of Ukraine with other law enforcement agencies in the field of combating cybercrime as one of the directions of ensuring the components of the security and defense sector. Topical Issues in Combating Cybercrime and Trafficking in Human Beings: Scientific and Practical Conference (Kharkiv, November 15, 2017. p. 21-24.

Law of Ukraine “On the Fundamental Principles of Cybersecurity of Ukraine” (2017). URL: https://zakon.rada.gov.ua/laws/show/2163-19

Law of Ukraine On Information (1992). URL: https://zakon.rada.gov.ua/laws/show/2657-12

Law of Ukraine “On the National Bank of Ukraine” (1999). URL: https://zakon.rada.gov.ua/laws/show/679-14

Law of Ukraine “On the Fundamental Principles of Cybersecurity of Ukraine” (2017). URL: https://zakon.rada.gov.ua/laws/show/2163-19
Constitution of Ukraine (1996). URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

Resolution of the Cabinet of Ministers of Ukraine “On Approval of the Regulation on the Ministry of Defense of Ukraine” (2014). URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF

Decision of the National Security and Defense Council of Ukraine of March 4, 2016 “On the Concept of Development of the Security and Defense Sector of Ukraine” (2016). URL: https://zakon.rada.gov.ua/laws/show/92/2016

Presidential Decree «On the Decision of the National Security and Defense Council of Ukraine of May 6, 2015» On the National Security Strategy of Ukraine (2015). URL: https://zakon.rada.gov.ua/laws/show/287/2015

Presidential Decree On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine» (2016). URL: https://law.gov.ua/laws/show/96/2016#n11

Fopoc G.B. Kondpasheva K.C. (2015) Information Society and Cyber Security. Cybersecurity in Ukraine: legal and organizational issues: materials in Ukraine. bp. conf. Clothes. 233 p.

Short biographical note about the contributors at the end of the article:

Olga VAKULYK, Candidate of Juridical Sciences, Associate Professor, National Academy of Internal Affairs
ORCID ID: orcid.org/0000-0003-3080-3165

Pavlo PETRENKO, Doctor of Law, ex-Minister of Justice
ORCID ID: orcid.org/0000-0003-2587-4412

Iulia KUZMENKO, Doctor of pedagogical sciences, Associate Professor, Kherson Faculty Odesa State University of Internal Affairs
ORCID ID: orcid.org/0000-0001-5471-6432

Maksym POCHTOVYI, Candidate of Juridical Sciences, Associate Professor, Kryvyi Rig Faculty of Dnipropetrovsk State University of Internal Affairs
ORCID ID: orcid.org/0000-0002-4312-7826

Ruslan ORLOVSKYI, Candidate of Juridical Sciences , Yaroslav Mudryi National Law University
ORCID ID: orcid.org/0000-0003-1752-6913