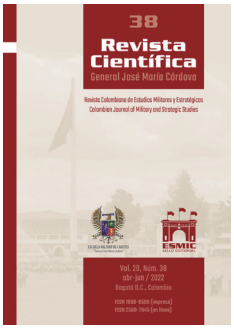

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

ISSN 1900-6586 (print), 2500-7645 (online)
Journal homepage: https://www.revistacientificaesmic.com

The system of cybersecurity bodies in Ukraine

Andrii V. Svintsytskyi
https://orcid.org/0000-0002-9801-0535
svintsytskyi19@neu.com.de
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of The Security Service of Ukraine, Ukraine.
University of the State Fiscal Service of Ukraine, Ukraine

How to cite in APA: Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. *Revista Científica General José María Córdova*, *20* (38), 287-305. https://dx.doi.org/10.21830/19006586.903

Published online: April 1, 2022

ESMIC
SELLO EDITORIAL
Miles Doctus

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 287-305
https://dx.doi.org/10.21830/19006586.903

The system of cybersecurity bodies in Ukraine

El sistema de organismos de ciberseguridad en Ucrania

Andrii V. Svintsytsky
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of The Security Service of Ukraine, Ukraine.
University of the State Fiscal Service of Ukraine, Ukraine

Abstract. This article describes Ukraine's cybersecurity system, its place, and its role in a single configuration of national security. The methods used include formal-dogmatic, comparative-legal, sociological, and hermeneutics. The research revealed that effective cybersecurity must be addressed comprehensively, requiring coordinated action at the national, regional, and international levels to prevent, prepare, and respond to incidents by the government, the private sector, and civil society.

Keywords: cyber defense; cybersecurity; cyberspace; cyber strategy; national security

Resumen. Este artículo describe el sistema de ciberseguridad de Ucrania, su lugar y papel en un complejo único de la seguridad nacional. Los métodos utilizados son el formal-dogmático, el comparativo-legal, el sociológico y el hermenéutico. La investigación reveló que la ciberseguridad efectiva debe ser abordada de forma integral, requiriendo una acción coordinada a nivel nacional, regional e internacional para prevenir, preparar y responder a los incidentes por parte del gobierno, el sector privado y la sociedad civil.

Palabras clave: ciberdefensa; ciberespacio; ciberestrategia; ciberseguridad; seguridad nacional

Section: Dossier • Scientific and technological research article
Received: November 30, 2021 • Accepted: February 12, 2022

Contact: Andrii V. Svintsytskyi ✉ svintsytskyi19@neu.com.de

Introduction

The law "On the Basic Principles of Cyber Security of Ukraine" (Law of Ukraine No. 2163-VIII, 2017) was adopted relatively recently, in 2017; however, the system of bodies addressing cybersecurity was formed long before. In 2007, the *State Special Communications and Information Protection Service (Derzhspetszviazok)* was established based on the dissolved Ukrainian Security Service's *Department of Special Telecommunication Systems and Information Protection* (Law of Ukraine No. 2163-VIII, 2006). It included the State's Special Communications Administration's *Department of Information and Telecommunication Systems Security*, later renamed the *State Cyber Protection Centre*.

In the same year, the *Computer Emergency Response Team* (CERT-UA) was established within the Department. Two years later, in 2009, this response team was accredited by the *Forum for Incident Response and Security Teams* (FIRST). In 2010, it became clear that the existing range of tasks was too considerable for one unit. Thus, two separate entities, part of the State's Special Communications Administration, were created based on the dissolved *Information and Telecommunication Systems Security Department*, namely, *the State Special Communications Information Security Department* and the *Special Information and Telecommunication Systems Department.*

In the same year, the former was renamed the *State Center for Information Resources Protection* (Boyarchuk et al., 2021). In 2012, developing international cooperation, CERT-UA received accreditation from the specialized security agency of the International Electrotechnical Commission (IEC), the *International Multilateral Partnership Against Cyber Threats* (IMPACT). In 2015, the need arose to regulate cybersecurity issues in Ukraine legislatively. Accordingly, the decision of the Board of the State Special Communications Administration[1] was adopted; it reorganized the State Special Communications Service's *State Center for Information Resources Protection* into the *State Cyber Protection and Countering Cyber Threats Centre* of the same State service.

The adoption of the law on the basic principles of cyber security (Law of Ukraine No. 2163-VIII, 2017) prompted a need to reorganize, restructure the staff, and redistribute the areas of responsibility of the *State Cyber Protection Centre* according to the law. The process lasted for two years. Finally, by decision of the Board of the State Special Communications Administration[2], the State's Special Communications' *Cyber Protection Centre and Countering Cyber Threats Centre* was reorganized into the *State Cyber Protection Centre of Special Communications and Information Protection Service* (abbreviated: *Center for Cyber Protection of the State Special Communications*). In 2019, the abbreviated

1 Decision of the Board of the State Special Communications Administration of 01/07/2015.
2 Decision of the Board of the State Special Communications Administration No. 01/01 / 01-3729 of July 26, 2018.

name was changed to the *State's Cyber Protection Centre of Special Communication and Information Protection Service* (SCPC).[3] In October 2020, a new edition of the *State Cyber Protection Centre of Special Communication and Information Protection Service* regulation was approved.[4]

According to the mentioned law on the basic principles of cyber security in the Verkhovna Rada of Ukraine (Law of Ukraine No. 2163-VIII, 2017), the main tasks of CERT-UA are as follows:

1. Collecting and analyzing data on cyber incidents, maintaining the State register of cyber incidents;
2. Providing practical assistance to the owners of cybersecurity objects on the prevention, detection, and elimination of cyber incidents on these objects;
3. Organizing workshops on cybersecurity concerning ensuring the national cybersecurity system and owners of cybersecurity objects;
4. Preparing and posting recommendations for combating modern types of cyberattacks and cyber threats on websites;
5. Interacting with law enforcement bodies, informing them promptly about cyberattacks;
6. Cooperating with foreign and international organizations on cyber incident responses, particularly concerning the participation of FIRST security incident response teams, including the payment of annual membership fees;
7. Collaborating with CERT-UA and other enterprises, institutions, and organizations carrying out activities related to cyberspace security regardless of ownership;
8. Processing information received from citizens on cyber incidents concerning cybersecurity objects;
9. Assisting State bodies, local governments, military formations established under the law, enterprises, institutions, and organizations regardless of ownership, as well as citizens of Ukraine in addressing cyber protection and combating cyber threats.

Structural units for combating cybercrime before the reformation

In 2010, cybercrime units appeared in the law enforcement bodies' structures. On the basis of the Ukrainian Ministry of Internal Affairs' *Department for Combating Crimes Related to Human Trafficking* and other relevant departments/units of the Ministry of Internal

3 Through order of the State Special Communications Administration No. 168 of March 25, 2019.
4 Through order of the State Special Communications Administration No. 686 of 26.10.2020.

Affairs of Ukraine in the Autonomous Republic of Crimea, oblasts of Ukraine, Kyiv, and Sevastopol, the *Department for Combating Cybercrime and Human Trafficking* was established, directly governing the units for combating cybercrime and human trafficking of the Ukrainian Internal Affairs bodies (Order No. 581, 2010).

According to its regulation, the *Department for Combating Cybercrime and Human Trafficking* was an independent structural unit of the Central Office of the Ministry of Internal Affairs of Ukraine, authorized to carry out operational and investigative activities. The Department carried out its activities on a linear and zonal principle based on a combination of unity of command and collegiality, long-term and current planning, considering scientific recommendations and best practices, including international. Following the mentioned regulation, the Department's primary operational and service tasks were the following:

- Providing organizational and practical support in implementing State policy to prevent and combat crimes committed involving high information technology and telecommunications networks, human trafficking, illegal migration, crimes against morality, crimes in the field of employment abroad, illegal adoption, violation of the law procedure for transplantation of human organs or tissues, forcible donation, and counteraction to legalization (laundering) of proceeds from these crimes.
- Implementing organizational and practical measures to detect and stop organized groups and criminal organizations' criminal activity, primarily of a transnational nature, and individuals specializing in the commission of crimes, the detection and cessation of which falls within the competence of the Department, an organization of operative support of criminal cases of the specified category.
- Organizing subordinate units' operational and service activities to detect and stop crimes, ensuring the prosecution of organized group members or individuals committing these crimes, identifying areas of work and priorities for subordinate units, finding effective means and methods of implementing the tasks assigned to them, ensuring organizational and methodological support for their activities to detect and stop crimes of this category.
- Developing and taking measures to improve forms and methods of operational and investigative activities of subordinate units, providing them with practical assistance in organizing work to detect and stop crimes, and solving other operational and service tasks.
- Ensuring control over the activities of business entities in employment mediation abroad, tourism entities, marriage, modeling bodies, as well as information market and telecommunication services business entities and representatives of interested ministries or other central executive bodies.

- Establishing confidential cooperation according to the legislation of Ukraine voluntarily with individuals able to cover the illegal activities of organized criminal groups and persons involved in the commission of crimes.
- Considering and disseminating positive experiences on recommendations of foreign law enforcement bodies on the detection, documentation, and investigation of such crimes in the fight against crime, together with higher education institutions of the Ministry of Internal Affairs and the Prosecutor General's Office.
- Organizing interaction with the Ukrainian Parliament Commissioner for Human Rights, other-state, non-state institutions, and international organizations engaged in combating cybercrime and human trafficking. Participating in international, interregional meetings, conferences, and seminars on problematic issues related to these types of crimes. (Order No. 494, 2012).

As shown, the Department's area of work was quite excessive, which is not surprising, given its name, which combined the fight against cybercrime and human trafficking. Moreover, these areas were poorly interconnected, barring the fact that the crimes related to "trafficking in human beings" could use some computer technology, for example, placing ads on the Internet to buy/sell human organs or advertise intimate services. Evidently, the same technology could be used to commit other crimes. Therefore, it is not surprising that two years later, the *Department for Combating Cybercrime of the Ministry of Internal Affairs of Ukraine* and units for combating cybercrime in the Main Department of the Ministry of Internal Affairs and regional departments in the Ministry of Internal Affairs were established.

The Department for *Combating Cybercrime of the Ministry of Internal Affairs of Ukraine* (UBK in Ukrainian) was an independent structural unit within the criminal police of the Ministry of Internal Affairs, which, according to the legislation of Ukraine, ensured the implementation of State policy and operational and investigative activities. According to the Ministry of Internal Affairs of Ukraine's Order No. 988 of 30/10/2012, "On the Organization of the Department for Combating Cybercrime and units for combating cybercrime of the Main Department and regional departments of the Ministry of Internal Affairs" (Order No. 988, 2012), the UBK's main tasks were to participate in the creation and implementation of State policy to prevent and combat the following:

- Criminal offenses using computing machinery (computers), computer systems and networks, and telecommunication networks;
- The mechanisms of preparation, commission, or concealment of criminal offenses involving the use of computing machinery (computers), computer systems and networks, and telecommunication networks. These activities in-

clude payment systems and the circulation of illegal information through these means, as well as economic aspects like financial and trade transactions carried out through telecommunication networks or computer networks and countering prohibited economic activities in this area (e-commerce), the provision of telecommunication services, and fraud and money laundering of proceeds from the above criminal offenses.

- As stipulated by applicable law, assist other units of the Ministry of Internal Affairs in the prevention, detection, and termination of criminal offenses and pre-trial investigations.

Cybersecurity-ensuring bodies' competence delimitation

During the reform of the internal affairs bodies in 2015, the *Cyber Police Department* was established within the National Police of Ukraine. According to the regulation approved by the Ministry of Internal Affairs through Order No.85 of 10/11/2015, this Department is an interregional territorial body of the Ukraine National Police, which is part of its criminal police. According to the legislation of Ukraine, it is responsible for ensuring the implementation of State policy in combating cybercrime and organizes and carries out operational and investigative activities.

This regulation also defines the *Cyber Police Department's* main tasks. They include participating in creating and implementing State policy to prevent and combat criminal offenses and the mechanism of preparation, commission, or concealment involving the use of computing machinery (computers), systems, computer networks, and telecommunication networks. It also assists other units of the National Police in preventing, detecting, and stopping criminal offenses as stipulated by applicable law. The cyber police's tasks include:

- The employment of the State policy in combating cybercrime;
- Providing the public with early warning on new, emerging cybercriminals;
- Introducing software to systematize cyber incidents;
- Responding to foreign partners' requests, coming through the channels of the 24/7 Network of National Contact Points (Cyber Police of Ukraine, 2020).

According to the ex-Minister of Internal Affairs Avakov (2015), the purpose of the cyber police is to restructure and develop units of the Ukraine Ministry of Internal Affairs. Moreover, it is responsible for the training and operation of highly qualified specialists in expert, operational and investigative police units involved in combating cybercrime, able to apply the latest technologies at a high professional level in operational and service activities. In addition, it must ensure the gradual transformation of the current model into

an innovative human rights body, which will respond instantly to cybercrimes and cyber threats and, following best world standards, will carry out international cooperation to neutralize transnational criminal groups. Avakov (2015) explained the cyber police's seven main tasks:

1. Implementing State policy against cybercrime.
2. Countering cybercrime in the following contexts:

   Payment systems:

   - Skimming - illegal copying of the contents of the magnetic stripe tracks (chips) of bank cards;
   - Cash trapping - ATM theft of cash by installing a special retaining pad on the ATM tent;
   - Carding - illegal financial transactions using a payment card or its details, which are neither initiated nor confirmed by its holder;
   - Unauthorized debiting of funds (payment) from bank accounts using remote banking systems.

   E-commerce and business:

   - Phishing - extortion of logins and passwords to e-wallets, online auction services, money transfers, or exchanges from Internet users;
   - Online fraud - the seizure of citizens' funds through online auctions, online stores, websites, and telecommunications;

   Intellectual property:

   - Piracy - illegal distribution of intellectual property on the Internet;
   - Card sharing - providing illegal access to satellite and cable TV;

   Information security:

   - Social engineering - a technology of the management of people in the Internet space;
   - Malware - the creation and spread of viruses and malicious software;
   - Illegal content - content that promotes extremism, terrorism, drug addiction, pornography, the cult of cruelty, and violence;
   - Refilling - illegal substitution of telephone traffic.
3. Providing early warning to the public on the emergence of the latest cybercrime.
4. Introducing software to systematize and analyze information on cyber incidents, cyber threats, and cybercrimes.
5. Responding to requests from foreign partners received through the channels of the 24/7 Network of National Contact Points.

6. Training police officers in the use of computer technology for combating crime.
7. Participating in international operations and cooperation in real-time and ensuring the functioning of the network of contact points between 90 countries.

Cyber police personnel consists of re-certified employees of the Ministry of Internal Affairs' anti-cybercrime units, selecting only those meeting cyber police officer requirements. In addition, nationwide cyber police recruitment was held to select the best cybersecurity specialists on a competitive basis (Bezzubov et al., 2017; Vystavna et al., 2018). In 2012, the *Department of Counterintelligence Protection of the State's Interests in the Sphere of Information Security of the Security Service* (DKIB SBU in Ukrainian) was established within the Ukraine Security Service (Presidential Decree No. 34, 2012). The DKIB SBU is an operational unit of the Ukraine Security Service, the scope of which includes ensuring the State's information security. The Security Service's *Counterintelligence Protection of the State's Interests in Information Security Department* is responsible for the State's security in the information and cyber spheres. It coordinates and controls the activities of regional bodies and central departments units of the Security Service. Within the limits of its competence, it submits proposals on the issuance of acts binding on public administration bodies, enterprises, institutions, organizations, and citizens to the President of Ukraine (Bilous, 2019).

The Department was established and developed with the assistance of the NATO-Ukraine Cybersecurity Trust Funds; especially favored by the fund was the Cyber Security Situation Centre. The hardware and software for the Centre's functioning were received in July 2017 as part of the first stage of implementing of the NATO-Ukraine Trust Fund on Cyber Defense Agreement. The Centre's grand opening took place with the participation of the Head of the Security Service of Ukraine, V. Hrytsak, on January 25, 2018 (Press center of the Security Service of Ukraine, 2018). The main tasks of the Cyber Security Situation Centre are as follows:

- Preventing, detecting, stopping, and disclosing crimes against the peace and security of humankind committed in cyberspace;
- Carrying out counterintelligence and operative search measures aimed at combating cyberterrorism and cyber espionage;
- Carrying out confidential reviews of the preparation level of critical infrastructure facilities for possible cyberattacks and cyber incidents;
- Combating cybercrime, the consequences of which may threaten the vital interests of the State;
- Investigating cyber incidents and cyberattacks on State electronic information resources, critical information, and infrastructure;

- Ensuring the response to cyber incidents concerning State security (Novikovas et al., 2017).

From 2017 to 2018, the Centre's specialists recorded and averted more than 50 cyberattacks of varying degrees of sophistication, some of which could have been much worse than the notorious "Petya-A" (Klimchuk, 2018). There is a plan to introduce similar units in regional security bodies in addition to the central Cyber Security Situation Centre. The first regional Cyber Security Situation Centre was established in Dnipro in November 2018. Six months later, with the participation of the Deputy Head of the Security Service of Ukraine, Oleg Frolov, a regional cybersecurity center was opened in Odesa.

International cyberlearning took place on different cybersecurity subjects in preparation for the 2019 parliamentary elections in Kyiv. The training was organized within the framework of the EU "Strengthening Cyber Security in Ukraine before the Elections" project, supported by the Estonian Center of Eastern Partnership (ECEAP) in cooperation with CybExer Technologies. The purpose was to collect the latest European experience in securing electoral processes and information in cyberspace. The cyberlearning sessions were attended by both European cybersecurity experts and Ukraine representatives, including specialists of the Security Service of Ukraine, the State Service for Special Communication and Information Protection, the cyber police, and the Central Election Commission of Ukraine. The training's virtual infrastructure enhanced the experience of counteracting hackers in conditions as close as possible to real situations (Krupskyi et al., 2019).

Among the Security Service's *Counterintelligence Protection of the State's Interests in the Sphere of Information Security Department's* achievements is the discontinuation of a powerful hacker group in July 2019, conducted jointly with US partners. The criminal hacker group based in Ukraine provided virtual services to other computer criminals, effectively creating the conditions for them to carry out illegal activities on the Internet without hindrance. The Ukraine citizen, the group's organizer, acquired his first hacking experience in Moscow in the mid-2000s. In 2007, the group provided services to hackers from other countries via Ukrainian networks. A large data center located on the private territory near Odesa was discovered during operational activities and further investigative actions. According to the acting Head of the Ukraine State Security Service, M. Kuleshov, almost one and a half hundred servers with thousands of hacker resources were confiscated. Some of them remained encrypted, configured so as not to keep traces of criminal activity (Press center of the Security Service of Ukraine, 2019).

The most recent of Ukraine's cybersecurity bodies is the *National Coordination Center for Cybersecurity of the National Security and Defense Council*, established in 2016. In the same year, the *National Coordination Centre for Cybersecurity* regulation was approved (Decree No. 96/2016, 2016). According to this regulation, this Centre is a work-

ing body of the Ukraine National Security and Defense Council, with a wide range of tasks, including:

1. Analyzing:
   - The state of cybersecurity;
   - The results of the review of the national cybersecurity system;
   - The cybersecurity-ensuring individual's level of preparation to perform tasks on combating cyber threats and implementation of measures to prevent and combat cybercrime;
   - The state of financial and organizational support of programs and measures for implementing State policy in cybersecurity in Ukraine;
   - The fulfillment of the legislation requirements on the cyber protection of State electronic information resources, information, and critical information infrastructure, as well as the requirements for protection established by law;
   - Data on cyber incidents related to State information resources in information and telecommunication systems;
   - Staffing of the national cybersecurity system to propose improvements;
2. Participating in the development of sectoral cybersecurity indicators;
3. Forecasting and identifying potential and real threats in cybersecurity in Ukraine;
4. Developing conceptual principles and proposals for State cybersecurity to improve the effectiveness of measures to identify and eliminate factors posing potential and actual threats in cybersecurity, preparation of draft programs, and plans to prevent and neutralize them;
5. Generalizing international experience in cybersecurity;
6. Ensuring the development and implementation of information exchange mechanisms required for cybersecurity-ensuring organizations to respond to cyberattacks and cyber incidents and eliminate their factors and negative consequences;
7. Providing the operational, information, and analytical support of the National Security and Defense Council on cybersecurity;
8. Developing and submitting proposals to the National Security and Defense Council on:
   a. Determining Ukraine's national interests in cybersecurity, priority areas, conceptual approaches to the formation and implementation of State policy concerning safe cyberspace and its use in the interests of an individual, society, and the State;
   b. Implementing systemic measures to strengthen the security and defense capabilities of sector entities in the fight against military cyber threats, cyber espionage, cyberterrorism, cybercrime, and ensuring cyber protection of State

electronic information resources, the protection required by law, and critical information infrastructure;

c. Implementing measures to ensure cyber protection of critical infrastructure and the protection of technological processes in production in the real sector of the economy;

d. Improving the cybersecurity regulatory framework in Ukraine, in particular the legal regulation of the areas of responsibility of the security and defense sector, ensuring Ukraine's cybersecurity and the interaction mechanisms between them;

e. Ensuring the development of State information infrastructure;

f. Coordinating activities of the entities in the security and defense sector that ensure cybersecurity in Ukraine;

g. Assessing the mutually agreed deployment of the Ukraine Armed Forces' cybersecurity units, other military formations, and special purpose law enforcement bodies formed under the laws of Ukraine, ensuring their preparedness to perform tasks under martial law in states of emergency or crises that threaten Ukraine's national security;

h. Overseeing the actions by national security subjects to improve cooperation with international organizations in cybersecurity and ensure the protection of Ukraine's national interests at the international level;

i. Setting priorities for attracting international technical assistance in cybersecurity;

j. Implementing State support measures for scientific institutions and organizations of strategic importance to the State's cyber defense, conducting scientific research involving cybersecurity and cyber defense for the needs of national security and defense;

k. Increasing the effectiveness of the implementation of military and technical policy and cooperation in cyber defense;

l. Strengthening the State's cyber defense capabilities, transfer of the national communication system, strategic national automated control systems, government networks, communication and weapons control systems, information and telecommunication networks, and systems of military administration to operate in a special period, mobilization of additional resources for organizing operations in cyberspace;

m. Improving the creation of domestic software products to protect the State's information resources, including the national operating system and national antivirus software.;

9. Monitoring the development and implementation of national standards and technical regulations for information use and communication technologies, harmonized with EU and NATO standards;
10. Defining ways, mechanisms, and means of solving problems that arise during the State's cybersecurity policy implementation;
11. Ensuring control over the status of decisions of Ukraine's National Security and Defense Council on State cybersecurity issues, enacted by Presidential decrees;
12. Studying international experience concerning the creation and operation of national cybersecurity systems, their dissemination among organizations and institutions, and monitoring their implementation in Ukraine;
13. Participating in the organization and conduction of interethnic and interagency cyberlearning training and the development of relevant methodological documents and recommendations (Presidential Decree No. 242, 2016).

The investigation of cybercrimes is entrusted to the investigative units of the National Police (Law of Ukraine No. 4651-VI, 2012), and forensic support for the investigation is provided by units of computer and telecommunication examinations of forensic institutions in Ukraine.

Problematic issues in combating cyber threats in Ukraine

It should be noted that the concept of "cybercrime" is not laid down in Ukraine's Criminal Code; however, it appears in other regulations, in particular, in the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" (Law of Ukraine No. 2341-III, 2001). These crimes are combined in Section XVI: "Criminal offenses in the use of computers, systems, and computer networks, and telecommunication networks" in the Criminal Procedure Code of Ukraine. These crimes include the following:

- Article 361. Unauthorized interference in the work of computing machinery (computers), automated systems, computer networks, and telecommunication networks.
- Article 361-1. Creation for the use, distribution, or sale of malicious software or hardware.
- Article 361-2. Unsanctioned sale or distribution of information with limited access stored in computers, automated systems, computer networks or on data storage devices.
- Article 362. Unauthorized actions on the information processed on computing machinery (computers), automated systems, computer networks, or on the data storage devices by individuals with the right to access it.

- Article 363. Violation of operation rules of computing machinery (computers), automated systems, computer networks, or telecommunication networks or the order and rules of the information protection processed in them.
- Article 363-1. Obstructing the function of computers, automated systems, computer networks, or telecommunication networks through the mass dissemination of telecommunication messages.

As can be seen from the above articles of the Criminal Code, one of the Ukrainian legislation's problems is the lack of a clear definition of "cyberterrorism." Given the danger to the public posed by obstructing the State's critical information systems infrastructure, many scholars consider it necessary to legislate criminal liability for a new type of particularly dangerous crime –cyberterrorism. Instead, Art. 258 of the Criminal Code addresses responsibility for "classic" terrorism; therefore, the position on the introduction of a new *corpus delicti* is ambiguous.

Several arguments favor a separate crime because the means of committing "ordinary" terrorism and cyberterrorism can differ, and the instruments of these crimes and their preparation are miscellaneous (Britchenko et al., 2018). All this leads to several tactics of investigation, different types of examinations that need to be appointed, and different specializations of law enforcement officers (investigators, operatives, specialists, experts), among others. Thus, the idea of separating cyberterrorism as an individual crime is well-founded and validated.

In June 2015, the Parliamentary Assembly of the Council of Europe adopted Resolution 2070 (2015) on "Increasing cooperation against cyberterrorism and other large-scale attacks on the Internet." It calls on the Council of Europe member states to define cyberterrorism and establish accountability for its activities. Thus, several bills on amendments to the Criminal Code of Ukraine were prepared following this resolution (UNIAN, 2015).

The draft "On Amendments to the Criminal Code of Ukraine (on enhancing liability for cyberterrorism and cybercrimes)" No. 2328a of July 10, 2015, initiated by Myrnyy (2015), provides for part two of Art. 258 of the Criminal Code. It states:

> 2. The same actions committed repeatedly, or for a previous conviction by a group of persons or if they are connected with unauthorized intrusion into the work of electronic processing machines (computers), violating the law on automated systems, computer networks, or high-risk electric circuits or if they have caused significant property damage or other severe consequences –shall be punishable by imprisonment for a term of seven to twelve years with or without confiscation of property. (p.1; author translation)

Meanwhile, Article 361 was proposed, supplemented with new parts (three and four) stating the following:

> 3. Actions provided for in parts one or two of this article, if they involve unauthorized interference with the operation of electronic processing machines (computers), any act or omission in the operation of automated systems, computer networks, or electronic communications of high-risk telecommunication networks, which caused significant property damage or other serious consequences –shall be punishable by imprisonment for a term of seven to twelve years with or without confiscation of property.
>
> 4. The acts provided for in parts one, two, or three of this article, which caused the death of a person –shall be punishable by imprisonment for a term of ten to fifteen years or life imprisonment with or without confiscation of property. (pp. 1,2; author translation)

The bill of Ukraine "On Amendments to the Criminal Code of Ukraine on Establishing Liability for Cyberterrorism"[5] (Aryev, 2015) proposes introducing a new article in the Criminal Code of Ukraine, namely Article 258-6, Cyberterrorism.

> 1. Cyberterrorism, that is, the intentional attack on information processed by a computer, computer system, or computer network that endangers human life and health or leads to other serious consequences if such actions have been committed out of political motives, for violating public safety, intimidating the population, provoking a military conflict –shall be punishable by imprisonment for a term of five to ten years with or without confiscation of property.
>
> 2. The same acts performed repeatedly or by a group of persons by prior conspiracy shall be punishable by imprisonment for a term of seven to twelve years with or without confiscation of property.
>
> 3. The commitment of an act of cyberterrorism that has resulted in injury, trauma or death shall be punishable by imprisonment for a term of ten to fifteen years, or life imprisonment, with or without confiscation of property.
>
> 4. A person or group of persons who participated in the preparation of an act of cyberterrorism, but who voluntarily warned the law enforcement agency and if their actions led to the prevention of an act of terrorism, shall be released from criminal liability if their actions do not constitute another crime (pp. 3-5; author translation).

To date, the amendments to the Criminal Code of Ukraine have not been adopted. However, the criminalization of cyberterrorism through the amendment to the Criminal Code is extremely important. It will provide legislative protection to automated information and telecommunication systems. Moreover, it will protect State electronic registers and databases and critical national information infrastructure.

As Nizovtsev (2017) notes, both bills show shortcomings. According to Draft Law No. 2328a, there are amendments to the second part of Art. 258 of the Criminal Code, and parts three and four are added to Art. 361 of the same Code. At the same time, the adoption of the specified bill could produce a conflict between part two of Art. 258 and

5 No. 2439a of July 24, 2015.

part three of Art. 361 of the Criminal Code. Similarly, there could be a conflict between the proposed Bill No. 2439a's articles 258-6 and 361. According to the scientist, the optimal option is the introduction of parts three and four to Art. 361 of the Criminal Code, as provided by Bill No. 2328a. Furthermore, the concept of "cyberterrorism" should be enshrined in a separate regulation, for example, in Ukraine's Cybersecurity Strategy. It should be noted that Nizovtsev's (2017) proposal has, in fact, been partially implemented; the term "cyberterrorism" has been enshrined in a separate legislative act, namely, the Law of Ukraine "On Basic Principles of Ensuring Cyber Security of Ukraine." It provides the following definition: "Cyberterrorism is a terrorist activity carried out in cyberspace or with its use" (Gnatenko et al., 2020). Nevertheless, the allocation of cyberterrorism as a separate crime has not yet occurred.

These are not the only issues in countering cyber threats in Ukraine. As noted by Peresada and Hobby (2020), several factors hamper the effective functioning of the above services. The first one is the problem of coordinating law enforcement bodies and legal regulations concerning the bodies' areas of responsibility to avoid duplicating powers, procedures, and means of a comprehensive response to cybersecurity threats. Secondly, the prevention of these crimes is not sufficiently effective. The third one involves technical equipment. Orlov and Onishchenko (2014) note that the high level of cybercrime is due to several reasons. However, law enforcement bodies' are limited due to the lack of special technical equipment such as modern computer equipment and computer technology, knowledge and skills to detect and investigate cybercrime, tactics, and techniques, given the limited access to these modern methods, and overall deficient information culture.

Furthermore, they are faced with limited training covering a wide range of law enforcement bodies and judges to bring the perpetrators to justice and the victims' distrust of law enforcement bodies. Lastly, national legislation focuses mainly on cybersecurity and cyber defense concerning the State and public systems, including telecommunications, leaving technical and public information resources insufficiently protected and not in line with current trends in the fight against cybercrime. This effort requires the further expansion of law enforcement areas to include private computer networks and individual personal computers. There are no small or insignificant casualties in cyberwarfare; personal computer devices and networks can serve as a training ground to prepare for large-scale cyberattacks on government structures and livelihoods.

The issue of coordination and division of areas of responsibility is urgent. For example, when a cybercrime activity is detected, the *Department of Counterintelligence Protection of the State's Interests in the Sphere of Information Security* officers must provide the National Police investigators materials to further the operative support of the investigation. However, the National Police's structure has its own units with very similar functions – the cyber police.

Another significant problem is the insufficient number of highly qualified personnel; this applies to the cyber police staffing and the *Department of Counterintelligence Protection of the State's Interests in the Sphere of Information Security* (Shopina et al., 2020). In-depth knowledge is vital when investigating crimes involving the latest cyber technologies and should not be limited to merely specialized operatives and forensic experts. Modern information technology must also be understood by the investigator, prosecutor, and judge for an investigation to be effective. After all, without understanding the nuances of computer technology and their attackers' "hacking," the investigation can only be protracted for a long time or closed without bringing the perpetrators to justice.

Given the above, we propose creating specialized investigative units to investigate cybercrimes and the relevant units in the prosecutor's office. The specialization of judges would also be relevant. At the same time, the described vertical of specialized bodies do not require the same degree of independence as, for instance, the anti-corruption vertical (meaning the National Anti-Corruption Bureau, the Specialized Anti-Corruption Prosecutor's Office, and the High Anti-Corruption Court).

Another significant problem in ensuring cybersecurity in Ukraine is the lack of scientific research in this area (Ilchenko et al., 2021). On the state of implementation of the Cybersecurity Strategy, approved by Presidential Decree No. 96 (2016), the National Security and Defense Council's decision of May 14, 2021, concluded that certain indicators do not surpass 40 percent. Insufficient scientific support is considered one of the main reasons for this outcome. Mainly subjects of the security and defense sector took part in this strategy's implementation; other state bodies, scientific institutions, and the public were all but excluded. Thus, educational and scientific institutions were underrepresented in implementing tasks related to developing scientific potential and the spread of cyber literacy (Presidential Decree No. 447, 2021).

During the international scientific and practical conference "Countering Cyber Threats in the Modern Security Environment: Current Issues in Theory and Practice," organized by the Ukrainian Scientific and Research Institute of Special Equipment and the Security Service Forensic Expertise of the National Security and Defense Council, it was noted that research in cybersecurity in Ukraine has been of unsystematic and episodic nature in recent years. A significant number of scientific papers were limited to proclaiming the importance of cybersecurity without specific weighty proposals of engineering, technical, organizational, or other nature. Therefore, a joint effort was proposed between the Ukrainian Scientific and Research Institute of Special Equipment and the Forensic Expertise of the Security Service to introduce a platform for the continuous exchange of experience and achievements in cybersecurity (UTRPI, 2021).

Conclusion

An entire system of specialized bodies for cybersecurity has been created in Ukraine. In addition, non-specialized bodies are also involved; "ordinary" investigators carry out the investigation of cybercrime under the procedural supervision of the prosecutor's office. At the same time, there are several problems in ensuring cybersecurity in Ukraine. These are the lack of highly qualified personnel, the lack of cyber specialization of investigators and prosecutors, the inconsistencies of legislation with modern realities, the difficulty in organizing the interaction of the related entities mentioned, and the lack of research and development. As a way to solve these problems, we have proposed to create specialized investigative units and relevant units of the prosecutor's office to investigate cybercrimes and introduce the appropriate specialization of judges. Furthermore, to coordinate scientific developments, we proposed creating a platform for ongoing exchange of experience and achievements in cybersecurity –a cybersecurity research center– based on the Ukrainian Research Institute of Special Equipment and the Forensic Expertise of the Security Service of Ukraine.

Disclaimer

The author declares no potential conflict of interest related to the article.

Funding

The author does not report sources of funding for this article.

About the authors

Andrii V. Svintsytskyi is a Ph.D. in Law, Director of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, and Associate Professor at the Department of Criminal Law and Criminology of the University of the State Fiscal Service of Ukraine. Honored Lawyer of Ukraine.

https://orcid.org/0000-0002-9801-0535 - Contact: svintsytskyi19@neu.com.de

References

Aryev, V.I. (2015). *On Amendments to the Criminal Code of Ukraine on Establishing Liability for Cyberterrorism*. Bill No. 2439a (July 24, 2015). Verkhovna Rada of Ukraine. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183

Avakov, A. (2015). Cyberpolice (reforms). *Ukrainian Truth in social media.* https://blogs.pravda.com.ua/authors/avakov/561a92c183c27/

Bezzubov, D., Ihonin, R., & Diorditsa, I. (2017). Cyberthreats as a component of threats in the contemporary world (a legal aspect). *Journal of Advanced Research in Law and Economics, 8*(7), 2086-2093. https://doi.org/10.14505/jarle.v8.7(29).04

Bilous, I.A. (2019). *Socio-Legal Support of Information Security of Ukraine* [Abstracts by Kharkiv, December 2019, pp. 120-124]. Scientific seminar on information aggression of the Russian Federation against Ukraine. Kharkiv National University of the Air Force named after Ivan Kozhedub.

Boyarchuk, R., Khudyntsev, M., Lebid, O., & Trofymchuk, O. (2021). *Organizational and technical model of national cybersecurity and cyber protection*. CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2923/paper5.pdf

Britchenko, I., Monte, A. P., Kryvovyazyuk, I., & Kryvoviaziuk, L. (2018). The comparison of efficiency and performance of Portuguese and Ukrainian enterprises. *Ikonomicheski Izsledvania, 27*(1), 87-108.

Cyberpolice of Ukraine. (2020). *About the unit*. https://cyberpolice.gov.ua/contacts/

Gnatenko, K. V., Yaroshenko, O. M., Inshyn, M. I., Vapnyarchuk, N. M., & Sereda, O. H. (2020). Targeted and effective use of state and non-state social funds. *International Journal of Criminology and Sociology, 9*, 2861-2869. https://doi.org/10.6000/1929-4409.2020.09.350

Ilchenko, M., Uryvsky, L., & Osypchuk, S. (2021). The main directions of improving information and communication technologies in the global trends. In Ilchenko, M., Uryvsky, L., Globa, L. (Eds.) *Advances in Information and Communication Technology and Systems*. [Lecture Notes in Networks and Systems, vol 152]. Springer. https://doi.org/10.1007/978-3-030-58359-0_1

Klimchuk, A. (2018). *Information and Cyber Security in the Modern World: Experience of the SSU*. Liga.net. https://www.liga.net/politics/opinion/informatsionnaya-i-kiberbezopasnost-v-sovremennom-mire-opyt-sbu

Krupskyi, O. P., Dzhusov, O., Meshko, N., Britchenko, I., & Prytykin, A. (2019). Key sources when formulating competitive advantages for hotel chains. *Tourism, 67*(1), 34-46.

Law of Ukraine No. 2163-VIII. (2006). *On the State Service for Special Communications and Information Protection of Ukraine*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Law of Ukraine No. 2163-VIII. (2017). *On the Basic Principles of Cyber Security of Ukraine*, Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Law of Ukraine No. 2341-III. (2001). *Criminal Code of Ukraine*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2341-14#Text

Law of Ukraine No. 4651-VI. (2012). *Criminal Procedure Code of Ukraine*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Myrnyy, I.I. (2015). *On Amendments to the Criminal Code of Ukraine (on enhancing liability for cyberterrorism and cybercrimes)*. Bill No. 2328a (July 10, 2015). Verkhovna Rada of Ukraine. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55972

Nizovtsev, Yu.Yu. (2017). Regarding Legal Regulation in the Field of Counteraction to Unauthorized Interference in the Work of Information and Telecommunication Systems. *Forensic Bulletin*, 1(27), 54-62. http://elar.naiau.kiev.ua/bitstream/123456789/16433/1/Visnik_1-27-2017-54-62.pdf

Novikovas, A., Novikoviene, L., Shapoval, R., & Solntseva, K. (2017). The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues, 7*(2), 369-380.

Order No. 494. (2012). *About the organization of activity of Management of fight against cybercrime of the Ministry of Internal Affairs of Ukraine and divisions of fight against cybercrime GUMVD, UMVD*. Ministry of Internal Affairs of Ukraine. https://ips.ligazakon.net/document/view/mvs308?an=1&ed=2012_05_31

Order No. 581. (2010). *About the organization of activity of Department of fight against cybercrime and human trafficking of the Ministry of Internal Affairs of Ukraine and divisions of fight against cybercrime and human trafficking GUMVD, UMVD*. Ministry of Internal Affairs of Ukraine. https://zakon.rada.gov.ua/rada/show/v0581320-10#Text

Order No. 988. (2012). *About the organization of activity of Management of fight against cybercrime of the Ministry of Internal Affairs of Ukraine and divisions of fight against cybercrime GUMVD, UMVD*. Ministry of Internal Affairs of Ukraine. https://ips.ligazakon.net/document/view/mvs308?an=1&ed=2012_05_31

Orlov, O.V., & Onishchenko, Yu.M. (2014). Organizational and Normative-Legal Bases of Fight Against Cybercrime. *Public Administration: Improvement and Development*, *4*. http://www.dy.nayka.com.ua/?op=1&z=715

Peresada, O.M., & Hobby, Y.S. (2020). Legal and Organizational Problems of Combating and Combating Cybercrime. *Modern Problems of Legal, Economic, and Social Development of the State* [Thesis Add. International. Scientific-Practical Conf. (November 2020, pp. 152-153)]. Kharkiv: Ministry of Internal Affairs of Ukraine, Kharki National University of Internal Affairs.

Presidential Decree No. 242. (June 7, 2016). *On the National Cyber Security Coordination Center*. President of Ukraine Official website. https://www.president.gov.ua/documents/2422016-20141

Presidential Decree No. 34 (September 25, 2012). *On Amendments to the Decree of the President of Ukraine of March 27, 2005 No.1860.* President of Ukraine Official website. https://www.president.gov.ua/documents/342012-13995

Presidential Decree No. 447. (June 14, 2021). *Decree of the National Security and Defense Council of Ukraine of June 14, 2021 "On the Cyber Security Strategy of Ukraine."* President of Ukraine Official website. https://www.president.gov.ua/documents/4472021-40013

Presidential Decree No. 96. (February 15, 2016). *On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 on the Cyber Security Strategy of Ukraine*. President of Ukraine Official website. https://www.president.gov.ua/documents/962016-19836

Press center of the Security Service of Ukraine. (2018). *The head of the Security Service of Ukraine opened the Situational Center for Cyber Security*. https://sbu.gov.ua/ua/news/1/category/2/view/4318#.OD1o8ogT.dpbs/

Press center of the Security Service of Ukraine. (2019). *SBU jointly with foreign colleagues blocks activity of powerful hacker group* [video]. https://sbu.gov.ua/en/news/1/category/21/view/6281#.iPzWFbSO.dpbs

Resolution 2070. (June 26, 2015). *Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet*. Parliamentary Assembly. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21975&lang=en

Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: Legal and organizational support in leading countries, NATO and EU standards. *Journal of Security and Sustainability Issues, 9*(3), 977-992. https://doi.org/10.9770/jssi.2020.9.3(22)

UNIAN. (2015). The Council proposes to establish criminal liability for cyberterrorism. http://www.unian.ua/politics/1106141-u-radi-proponuyut-vstanoviti-kriminalnu-vidpovidalnist-za-kiberterorizm.html

UTRPI. (2021). *International scientific and practical conference "Countering cyber threats in the modern security environment: current topics of theory and practice."* June 1 to 31. Ukraine. https://utrpi.org.ua/mizhnarodnoyu-naukovo-praktychnoyu-konferentsiyeyu-protydiya-kiberzagrozam-u-suchasnomu-bezpekovomu-seredovyshhi-aktualni-pytannya-teoriyi-ta-praktyky-zavershyvsya-misyats-kiberbezpekyyakyj-z-1-po-31/

Vystavna, Y., Cherkashyna, M., & van der Valk, M. R. (2018). Water laws of Georgia, Moldova and Ukraine: Current problems and integration with EU legislation. *Water International, 43*(3), 424-435. https://doi.org/10.1080/02508060.2018.1447897