Countering Cybercrime Under Martial Law

Ruslan Orlovskyi*, Sergiy Kharytonov, Igor Samoshchenko, Olha Us and Volodymyr Iemelianenko

Department of Criminal Law Policy, Yaroslav Mudryi National Law University, Kharkiv, Ukraine
E-mail: rs.10@ukr.net
**Corresponding Author*

Received 23 June 2023; Accepted 31 August 2023;
Publication 17 November 2023

Abstract

To date, it is impossible to imagine your life without all kinds of gadgets, the Internet and social networks. The active using of social networks has long been carried out by all state bodies in order to cause confidence of the population to their actions, to see feedback in the format of comments, as well as to show people all topical processes. It is also important to note that Ukraine is an advanced state in the field of electronic document circulation, and therefore almost all processes, starting from the activities of banking institutions and ending with the activity of air and railway transport are carried out by automated electronic systems. Accordingly, the coordinated and uninterrupted functioning of all of the above is due to the stability of cyberspace. In connection with Russia's attack the information space became the second battlefield. Cyberattacks and official state sites hacking was immediately started, there were active attempts to abduct electronic data of banking institutions and private enterprises. The relevance of this article is determined by it, because a detailed analysis of the characteristic features of cybercrime, the search for methods and mechanisms of countering cybercrime in the conditions of war are the primary tasks and contribution to victory. The purpose of the article is to analyze the current state of countering cybercrime and

Journal of Cyber Security and Mobility, Vol. 12_6, 893–910.
doi: 10.13052/jcsm2245-1439.1264

varieties of cybercrime, to identify features and characteristics of cybercrime, as well as to make proposals for improving the current legislation in this area. The study used the following methods: analysis and synthesis, legal, static, systemic and formal-legal methods, method of interpretation of law. The conclusions, which we will make, can be a basis for further improvement of legislation, research and discussions between theorists and practitioners.

Keywords: Cybercrime, countering cybercrime, martial law, cyberspace, cyberattack.

1 Introduction

New realities are characterized by new challenges. The active use of information technologies and their rapid development led to the emergence of cybercrime. The idea of a thief was also transformed under the influence of the information revolution. Today, anyone who has a gadget and access to the Internet can be a cyber-criminal, as most computer processes do not require deep technical knowledge. During Russia's war against Ukraine, such a person can become a dangerous weapon in the hands of the aggressor country, as stolen electronic data can cause damage to Ukraine's state security and undermine its defense capability. In the conditions of war, cybercrime is generally carried out in order to destabilize the situation in the country, spread panic and misinformation among the population. In addition, when we talk about cybercrime in martial law, it should also be noted that cyberattacks are possible not only from Russia, but also those who simply use the vulnerable position of the state. Such situations clearly manifested when law enforcement agencies are loaded with different cases and sometimes overloaded, which causes a lack of time and resources to respond rapidly to an offense in this area [1].

The Constitution of Ukraine stipulates that protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security shall be the most important functions of the State and a matter of concern for all the Ukrainian people [2]. Ensuring information security and countering cybercrime is an important process of preserving the integrity of the state, its functioning and defense capability. The concept of "cybercrime" first appeared in American literature in the early 1960s. Cybercrime or computer crimes were first characterized at the Conference of the American Advocacy Association in Dallas in 1979. The main features of computer crimes include the following: (a) the use of a computer (computers) or other

computing system in the unlawful activities under the cover of erroneous promises or unreasonable reasons regarding receiving an illegal benefit in the form of funds, services or objects of ownership; (b) availability of deliberately unauthorized action, which is carried out to destroy, change or damage your computer, operating and/or computer system, programs, networks or information, etc.; (c) deliberately unauthorized dysfunction of computers and all kinds of systems or networks [3].

In the context of our research, it is worth examining international legal documents in the field of countering cybercrime, because the provisions of these documents can contribute to improving the legislation of Ukraine in the conditions of martial law. First of all, it is necessary to indicate the Council of Europe Convention on Cybercrime, which is the primary international treaty which deals with cybercrime. The convention provides for the application of a number of rules related to countering cybercrime and, in particular, calls on states to ratify and ensure effective cooperation of international services in the investigation of cybercrimes [4]. Within the framework of the eleventh and twelfth Congresses of the organization on crime prevention and criminal justice (UN Congress on Crime Prevention and Criminal Justice), the problems of international partnership in the war against cybercrime were discussed. Measures to strengthen international partnership and improve state legislation in the field of drug trafficking, the fight against money laundering, terrorism, and cybercrime were discussed. The UN has put computer crimes on the same level as terrorism, which indicates a special interest in this issue from the world community [5].

The activities of the European Union in the field of combating cybercrime are aimed at early detection and active response to manifestations of cybercrime. The main documents adopted to counter illegal encroachments on electronic information resources are the EU Directive on countering cyberattacks on information systems and the European Commission Directive on combating fraud and other financial crimes on the Internet. In turn, the Cybersecurity Strategy of the European Union adds new wording to the concept of "cyber protection", such as the detection and blocking of cyber-attacks, the localization of their consequences regardless of their origin in relation to civilian objects of all forms of ownership, as well as the detection and investigation of cybercrimes [6].

For the purposes of our research, it is necessary to define, first of all, the concepts of "cybercrimes" and "cybercrime" in national legislation. According to the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" cybercrime (computer crime) – a socially dangerous criminal

act in cyberspace and/or with its use, the liability for which is provided by the law of Ukraine on criminal liability and/or which is recognized as a crime by the international treaties of Ukraine. This law also defines that the cybercrime – a set of cybercrimes [7]. In turn, the Criminal Code of Ukraine provides for liability for criminal offences related to the use of electronic computing machines (computers), systems and computer networks and telecommunication networks [8]. At the same time, the Criminal Code of Ukraine does not contain the concept of cybercrimes or cybercrime.

At the same time, it is important to note that modern scientific research on cybercrime in the conditions of martial law, although being carried out, has not yet given a full answer to all the complex questions related to this problem [9]. One of the areas of research is the development and implementation of new technologies and methods of protection against cybercrime, in particular in the conditions of martial law. Such studies are aimed at the development of effective systems of control and monitoring of computer networks, protection of information from unauthorized access. Another important area of research is the analysis and classification of typical cybercrimes that may occur in martial law. Such studies make it possible to develop effective strategies for combating cybercrime and to ensure the maximum level of cyber security in the conditions of a military conflict [10].

The implementation of martial law became a catalyst for improving the regulation of relations in the information space. Before the beginning of the large-scale invasion, the issue of countering cybercrime and its legislative regulation was in its development stage and needed to be updated. It is due to the rapid development of information networks and the inability of various control mechanisms to adapt to such rapid changes.

2 Methodological Framework

In the course of the study, the following general scientific and special methods of scientific research were used. Legal and statistical method, which show the effectiveness of measures taken by country to ensure the realization of measures aimed at countering cybercrime in martial law. The systematic method is used to consistently study national norms on countering cybercrime and the influence of international experience on the implementation of mechanisms for such countering. The formal-legal method consists in analyzing the norms of national legislation to ensure the realization of measures aimed at countering cybercrime in martial law. Methods of analysis and synthesis are necessary to develop proposals for further improvement of the rule-making

regulation of mechanisms for countering cybercrime. It also used the method of interpretation of law, which revealed certain patterns of formation of the concept of "cybercrime" and its functioning.

The use of these methods will allow to make a comprehensive study of the problem of countering cybercrime, as well as provide an opportunity to make some theoretical generalizations and formulate scientific and practical conclusions. The empirical basis is the Constitution of Ukraine and the laws of Ukraine, as well as international normative legal documents.

The problem of countering and overcoming cybercrime is the object of research by such scientists as: Pushkarenko [3], Holovkin et al. [11], Shevchuk et al. [12], Wadovskyi [13], Yatsyshyn [14], Zabara [5], Movchan [15], Leghan [16], Dibrova et al. [17], Hloviuk and Zavtur [18], etc.

3 Results and Discussions

The rapid development of information technologies and global computerization have provided us with great opportunities for growth and development, and at the same time have caused the emergence of a new type of crime, better known as cybercrime. Cybercrimes have become a phenomenon which develop no slower than information technology itself. Therefore, the reaction of state bodies in the form of countering cybercrime should be no less rapid.

The legislative framework which exists in Ukraine for countering cybercrime includes the following legal acts. Firstly, the Criminal Code of Ukraine, which defines criminal offenses in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks and establishes criminal liability for such acts [8]. Martial law conditions can affect the nature and scope of criminal liability for cybercrimes. Secondly, the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" contains the main principles and directions of activity in the field of cyber security in the state, and also establishes requirements for the protection of information and information systems from possible cyber-attacks [7]. Thirdly, the Law of Ukraine "On Personal Data Protection", which regulates relations related to the protection and processing of personal data and is aimed at protecting the fundamental rights and freedoms of a person and a citizen, in particular the right to non-interference in personal life, in connection with the processing of personal data [19]. Fourthly, the Law of Ukraine "On Information". In its provisions, this Law defines the rights and obligations regarding access to information, as well as establishes requirements for the protection of information from unauthorized

access and use [20]. The Decree of the President of Ukraine "On the Introduction of Martial Law in Ukraine" and the Law of Ukraine "On Approval of the Decree of the President of Ukraine "On the Introduction of Martial Law in Ukraine", which were adopted in the context of the full-scale invasion, are also important for regulating the social relations we have outlined.

The full-scale invasion of the Russian Federation on the territory of Ukraine was accompanied not only by massive missile attacks, but also by a huge number of hacker attacks. On February 23, 2022, a cyber-attack on the banking system of Ukraine and state resources was recorded [21]. On the same day, the websites of the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, the Security Service of Ukraine, and the Ministry of Foreign Affairs of Ukraine were attacked [22]. As a result, these sites contained "messages" from the Russians about the reasons for their attack and, as it was, revenge for historical events a century ago. At the same time, the "Diya" application portal withstood the attack and saved the personal data of Ukrainians. The Ministry of Education and Science of Ukraine independently closed access to its website in order to prevent the actions of intruders. On February 24, 2022, the site of the Kyiv Regional State Registration suffered a hacker attack, while a significant number of the site's resources were disconnected in time to save information [23]. However, not only the websites of state bodies were the target of cyber-attacks. Mass mailings with phishing links to personal e-mail addresses of servicemen, their family members and related persons were also discovered [24]. These are just a few examples of cybercrime on a large scale. Much more crimes are committed against ordinary citizens in order to get hold of their personal data, and martial law has opened up more opportunities for it.

Due to such active actions of the Russian Federation not only on the real battlefield, but also on the information battlefield, the state was forced to actively counter hacker attacks. At the same time, perpetrators were often not only citizens of other states, but also citizens of Ukraine, who aimed to take advantage of the vulnerable position of the state and its citizens. That is why the Verkhovna Rada of Ukraine started working on improving the mechanism of countering cybercrime and strengthening responsibility for such actions.

The result of such activity was the optimization of the current legislation and the improvement of the grounds and procedural mechanisms for bringing cybercriminals to criminal liability. Changes are concentrated in two laws: "On amendments to the Criminal Procedure Code of Ukraine" [25] and the Law of Ukraine "On Electronic Communications" regarding increasing the effectiveness of pre-trial investigation "on hot tracks" and countering

cyber-attacks" and "On amendments to the Criminal Code of Ukraine to increase the effectiveness of the fight against cybercrime in the conditions of martial law" [26].

Provisions of the Law of Ukraine "On amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Electronic Communications" regarding increasing the effectiveness of pre-trial investigation "on hot tracks" and countering cyber-attacks contain changes to many institutions of criminal proceedings (status of documents as a source of evidence, fixation of criminal proceedings, measures to ensure criminal proceedings, investigative (search) and covert investigative (search) actions, special regime of pre-trial investigation and prolongation of detention during court proceedings under martial law, state of emergency or in the area of anti-terrorist operation or measures to ensure national security and defense, etc.) and respectively aimed at simplifying the order of gathering and verifying evidence [26]. It should be noted that some changes require additional analysis of proportionality of intervention in the aspect of human rights restriction. Most of the changes provided for by this Law contain general, not special (in the conditions of martial law) norms and touches not only countering cybercrime, but also other legal relations [18].

This law has a particular importance for us precisely in the aspect of the amendments of the means of countering cybercrime. So, it is worth highlighting such changes:

- ability to arrest on computer systems or on their separate parts, if they are a means of committing a criminal offense or receiving them is the end result of an offense;
- ability to arrest on computer systems or on their separate parts if they are required for research by an expert;
- introduction of a new investigative action for criminal proceedings, such as taking data of technical devices and technical means that have the functions of photo, film, video recording or photo, film, video recording means;
- the possibility for investigators to obtain access to mobile networks, computer systems or their individual parts during a search without prior authorization, only if the information obtained as a result of such actions has a significant importance for establishing the circumstances of the offense [26].

Regarding the Law of Ukraine "On amendments to the Criminal Code of Ukraine to increase the effectiveness of the fight against cybercrime in the

conditions of martial law", then its provisions are primarily aimed at optimizing the state cybersecurity system in order to actively counteract cyber threats both from other states and from the citizens of Ukraine; introduction of much more effective mechanisms and ways of counteracting cybercrime, as well as ensuring reliability and safety in the process of using digital services [25]. These updates also provide that interference with the operation of electronic communication, information, communication systems, electronic communication networks will not be considered illegal if it is carried out on the basis of the Procedure of search and identification of potential vulnerability of such systems or networks.

The above-mentioned Procedure is being finalized by the State Service of Special Communications and Information. Its adoption will be important for countering and combating cybercrime, as it will require testing of all state information systems by professionals. The text of this document provides for the creation of a national IT community Bug Bounty, which will be able to legally check all systems and identify their vulnerabilities. Accordingly, the state will have in its arsenal an effective tool for countering cybercrime and increasing the degree of protection of various types of information systems. As part of our research, it is also worth analyzing the types of offenses in the information space, which will help to form an idea about further steps to improve the mechanism of countering cybercrime.

The Convention on Cybercrime, which has been ratified by the Verkhovna Rada of Ukraine and therefore is a part of national legislation, identifies four main types of cybercrime, namely [4]:

(1) offenses against the confidentiality, integrity and availability of computer data and systems (such offenses include illegal interception of data, illegal access, data interference and system interference, misuse of devices);
(2) offenses directly related to computers (such offenses include fraud and forgery related to computers);
(3) offenses related to content (such offenses related to child pornography);
(4) offenses related to violation of copyright and related rights.

The most common types of cybercrime today are:

– carding – is a type of cybercrime which involves fraudulent credit card transactions that are not authorized by the cardholders;
– phishing – is a type of carding, which is a fraudulent activity which involves luring card details from the cardholder. The peculiarity of phishing is that the cardholder voluntarily shares this data with the

attacker, not realizing the consequences of his actions. There are two types of phishing: SMS phishing (such actions are carried out by means of messages about the alleged blocking of the card and the need to obtain card details for its further unblocking; although this is not the only example, as attackers go beyond traditional forms of SMS phishing) and Internet phishing (when fraudsters create fake pages which imitate the official pages of banks, payment services, online stores, etc.; in this case, cardholders do not check the name of the site and therefore thoughtlessly enter card details);

- vishing – carried out according to the phishing scheme, but with the help of phone calls;
- skimming – copying payment card data using a special device. In general, it is performed during ATM transactions using mini-cameras or a removable keyboard;
- shimming – an improved type of skimming, in which the copying of the card data in the ATM is carried out inconspicuously using a device placed inside the card reader;
- online fraud – creation of fake websites, online stores, etc.;
- piracy – unlawful and illegal distribution of intellectual property objects on the Internet;
- malware – the creation and subsequent distribution of dangerous viruses and similar malicious software;
- illegal content – information which contains calls for terrorist actions, extremism, drug addiction, pornography and the cult of cruelty;
- hacking of various sites, web pages in order to obtain personal data, corporate data, data constituting state or commercial secrets [27].

Martial law conditions can contribute to an increase in cybercrime, as such conditions often lead to increased chaos and instability in society [15]. The main types of cybercrimes under martial law, along with the above, include:

- cyberespionage – manifests itself in the form of illegal access to information related to the national interests and security of the country, its defense capability;
- cyber terrorism – manifests itself in the form of hacker attacks on water supply networks, electricity networks, medical systems, banking systems, etc. Such attacks cause interruptions in the functioning of the country's usual life and, accordingly, have both negative financial consequences and affect the country's security situation [16];

- cyber war – is an analogue of traditional war in cyberspace (which we can observe now as a result of the attack of the Russian Federation on Ukraine). Cyber war involves cyber-attacks on military facilities, including weapons storage facilities and cyber command. However, the elements of cyber war also include attacks on the systems of banking institutions, medical institutions, energy systems, etc.;
- misinformation – the spread of fake news which is intended to sow panic, worsen communication between society and the government, undermine citizens' trust in state bodies, and divert attention from real threats. It is generally done through mass media and social networking sites.

Our analysis of current national legislation and key international documents, as well as the characteristics of the main types of cybercrimes both in wartime and peacetime conditions, allows us to formulate the following ways of countering cybercrime. Firstly, it is necessary to form a national cyber security strategy, which will contain tactical and strategic priorities and tasks in this area. It also involves the creation of legislation which will be able to cover the entire range of relations in the information space. Accordingly, the norms should also regulate the issue of monitoring compliance with legislation in this area. Secondly, a very important step is to ensure the cyber security of important infrastructure facilities, namely power plants, water intakes, hospitals, etc. These objects must be protected from cyberattacks, because their functioning directly affects the life of the entire state. To do this, you should encrypt data, make backup copies, perform network protection and intrusion detection, install programs which will detect and neutralize viruses [28]. Thirdly, all information systems, without exception, must have the latest software which is tested by professionals and has a multi-level level of protection. Moreover, all systems must be constantly updated and backed up. It should be done to prevent data leakage.

In the context of martial law, counter-intelligence in the information space will be effective in countering cybercrime in order to identify third-party intrusions into the network and the persons who carry out it. In addition to the direct perpetrators, it is also necessary to identify the persons who are the customers of such "services". This activity should be carried out in order to prevent illegal access to data and eliminate the consequences. In order to actively counteract cybercrime, law enforcement agencies should also be established to combat cybercrime. They must have an appropriate level of knowledge and training, as well as adequate support for their activities.

An important step is cyber defense of the military sphere, because by obtaining data of military importance, the war can be won not only in the information field, but also in the real one. Therefore, the primary task is to ensure a high level of cyber defense of military systems, including military emails, communication networks, military databases, etc. A fairly effective way to counteract cybercrime is to improve the qualifications of employees and conduct additional training and cybersecurity training. Under such conditions, the staff will be able to prevent or detect a real cyber threat [17].

It should also be carried out a great work to increase the cyber awareness of the population, as well as provide basic knowledge on safe behavior in social networks and when visiting sites. For example, for your own safety, you should not open emails from strangers and follow links from them; it is appropriate to compare the domain names of well-known sites with those you want to visit; it is worth using licensed software; not to share passwords, access codes and bank card data with third parties; check information only from official websites or official phone numbers; use an antivirus; use different complex passwords for different sites and social networks, etc. [13].

Cybercrime is a phenomenon which has no borders, so it can easily go beyond attacks on the information space of Ukraine and spread to other states. Therefore, it is necessary to carry out active international cooperation in the field of identifying potential threats, their elimination and so on. Now we can actively observe such a method of countermeasures, when various states provided assistance in the field of cyber defense to Ukraine in order to speed up the victory.

Combating cybercrime in the conditions of martial law should be carried out with the help of modern technologies and methods of protection. They include:

- the use of artificial intelligence technologies, which will allow early detection of potential threats and their neutralization;
- the use of cyber-physical systems to protect critical infrastructure. These systems are necessary to control the parameters of technological processes, as well as the environment [14];
- use of blockchain technology;
- use of cyber security tests to identify weak points in software;
- multi-step authentication, which is carried out using voice recognition, fingerprints or face scanning. This method prevents the use of fake data.

Based on the above, it can be said with confidence that countering cybercrime in the conditions of martial law is a rather important, necessary

and at the same time difficult task facing Ukrainian society. State authorities are already working on improving legislation in the field of cyber security, but the actions of each citizen are equally important.

4 Conclusions

The level of state development in the 21st century is determined not only by economic and military power, but also by the level of development of countering cybercrime and ensuring the protection of the information space. New challenges associated with active computerization and the introduction of the latest technologies bring with them new problems and threats. Many politicians increasingly use the methods of information warfare to achieve their goals. A vivid example of this was the Russian-Ukrainian war, which brought not only human losses, damage to infrastructure, but also massive cyber-attacks on state resources and disinformation.

Improving the effectiveness of the countering and combating cybercrime in time of war and strengthening liability for relevant crimes is a long overdue step. The innovations in the regulation of legal relations to combat cybercrime which we have analyzed make it possible to assert that increased liability and expanded powers of law enforcement agencies in the investigation of cybercrime can partially deter potential criminals from committing new crimes.

The introduction of liability for crimes committed under martial law is also justified. The increased severity of sanctions for their commission is due to the current situation in the country. A person who harms the national interests and security of Ukraine and its citizens in cyberspace automatically assists the aggressor in this war, and therefore cannot be held less responsible than war criminals.

That is why Ukraine should not stop on the way to building a complete cyber security system. It is worth monitoring information security, protecting critical infrastructure, using the latest technologies and artificial intelligence to effectively protect the information space, encrypting data, etc. The need for this one is especially felt in the military sphere, since cybercriminals in the conditions of martial law carry out their attacks mostly on military objects. There should also be active cooperation between state authorities, society, IT specialists, military structures, and private enterprises to improve the mechanism for countering cybercrime.

In addition, training and professional development of employees of various services should be carried out. Institutions of higher education should

update their curricula and include a subject on cyber protection and security in the information space in order to reduce the likelihood of falling into the hands of attackers.

It is worth noting that all efforts to counter cybercrime under martial law must be based on international standards and legislation, as well as ensure the protection of human rights and fundamental freedoms. National legislation, in turn, must adapt to international legal norms and modern requirements.

Thus, based on our research, it is safe to say that countering and combating cybercrime remains an important vector of activity of the state and the international community. In the context of martial law, the use of the latest technologies and modern methods helps to increase the effectiveness of countering cybercrime and reduce the negative consequences of the offenses committed.

References

[1] K. Orobets, 2022. Concept, signs and types of criminal offence in legislation and practice of the US and Ukraine. Pakistan J. Criminol. 14(2): 47–62.

[2] Constitution of Ukraine, 1996. Available: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80?lang=en#Text.

[3] P. Pushkarenko, 2006. Cybercrime as a new phenomenon of the shadow economy. Probl. Prosp. Dev. Banking Syst. Ukraine. 17: 75–82.

[4] Convention on Cybercrime, 2001. Available: https://zakon.rada.gov.ua/laws/show/994_575#Text

[5] I. Zabara, 2012). International legal regulation of cooperation of states in the fight against information crime. J. Acad. Advoc. Ukraine. 17: 1–6.

[6] Cybersecurity strategy of the European Union: an open, safe and secure cyberspace, 2013. Available: http://www.enisa.europa.eu.

[7] Law of Ukraine No 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine", 2017. Available: https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text.

[8] Criminal Code of Ukraine, 2001. Available: https://zakon.rada.gov.ua/laws/show/en/2341-14#Text.

[9] R. Orlovskyi, O. Us, V. and Shevchuk, 2022. Committing a criminal offence by an organized criminal group. Pakistan J. Criminol. 14(2): 32–45.

[10] V.V. Haltsova, S.O. Kharytonov, O.M. Khramtsov, O.O. Zhytnyi, and A.A. Vasyliev, 2021. Criminal law as a means of protecting human rights

and freedoms in the modern world. J. Natl. Acad. Leg. Sci. Ukraine. 28(3): 248–256.

[11] B.M. Holovkin, O.V. Tavolzhanskyi, and O.V. Lysodyed, 2021. Corruption as a cybersecurity threat in the new world order. Connect.: Q. J. 20(2): 75–87.

[12] V. Shevchuk, V. Vapniarchuk, I. Borysenko, D. Zatenatskyi, and V. Semenogov, 2022. Criminalistic methodics of crime investigation: Current problems and promising research areas. Rev. Jurid. Portuc. 32: 320–341.

[13] V. Wadovskyi, 2021. Cybercrime in Ukraine: the most common crimes and how citizens can take care of their own information security. Law. L. 8. Available: https://equity.law/press-center/publications/1169.html.

[14] S. Yatsyshyn, 2018. Cyber-physical systems and their software. Meas. Tech. Metrol. 79(1): 34–38.

[15] R. Movchan, 2022. Analysis of legislative changes aimed at improving the effectiveness of criminal law countering cybercrime in wartime conditions. Leg. Sci. Electron. J. 5: 494–498. doi:10.32782/2524-0374/2022-5/118.

[16] I. Leghan, 2021. Features of international cooperation regarding the prevention and fighting of cybercrime and cyber terrorism. Sci. Bull. Int. Humanitarian Univ. Jurisprud. 50: 118–121.

[17] T. Dibrova, D. Pisenko, and N. Smetanina, 2022. Cybercrime and cyberfraud under martial law. Leg. Sci. Electron. J. 11: 546–549. doi:10.32782/2524-0374/2022-11/132.

[18] Hloviuk, I., & Zavtur, V. (2022). Law of Ukraine "On amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On electronic communications" on improving the effectiveness of pretrial investigations "in hot pursuit" and counteracting cyberattacks" No. 2137 – IX: analysis of criminal proceedings. Higher School of Advocacy of HSA, 1–13.

[19] Law of Ukraine No 2297-VI "On Personal Data Protection", 2010. Available: https://zakon.rada.gov.ua/laws/show/en/2297-17#Text.

[20] Law of Ukraine No 2657-XII "On Information", 1992. Available: https://zakon.rada.gov.ua/laws/show/en/2657-12#Text.

[21] State Service of Special Communication and Information Protection of Ukraine, 2022. Another cyberattack to state bodies and banks. Available: https://cip.gov.ua/ua/news/chergova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki.

[22] Ukrinform, 2022a. Sites of Banks and Authorities have undergone a mass DDOS-attack. Available: https://www.ukrinform.ua/rubric-tec

hnology/3410542-sajti-bankiv-ta-organiv-vladi-zaznali-masovoi-ddosataki.html.
[23] Ukrinform, 2022b. Hackers are attacking the site of the Kyiv Regional State Administration. Available: https://www.ukrinform.ua/rubric-technology/3411812-sajt-kiivskoi-oda-atakuut-hakeri.html.
[24] Ukrinform, 2022c. Email addresses of the Ukrainian military are being attacked by hackers. Available: https://www.ukrinform.ua/rubric-technology/3412829-emailadresi-ukrainskih-vijskovih-atakuut-hakeri.html.
[25] Law of Ukraine No 2149-IX "On amendments to the Criminal Code of Ukraine to increase the effectiveness of the fight against cybercrime in the conditions of martial law", 2022. Available: https://zakon.rada.gov.ua/laws/show/2149-20?lang=en#Text.
[26] Law of Ukraine No 2137-IX "On amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Electronic Communications" regarding increasing the effectiveness of pre-trial investigation "on hot tracks" and countering cyber-attacks", 2022. Available: https://ips.ligazakon.net/document/view/T222137?an=1.
[27] Yu. Gazizova, 2020. Cybercrime in Ukraine. The era of digital technologies is the era of new crimes. Law. L. 12. Available: https://uz.ligazakon.ua/ua/magazine_article/%20EA013606.
[28] M. Burdin, Yu. Gnusov, and S. Kalyakin, 2018. Certain aspects of combating new generation cyber-attacks. In: Actual Issues of Combating Cybercrime and Human Trafficking: Proceedings of the All-Ukrainian Scientific and Practical Conference (pp. 23–26). Kharkiv National University of Internal Affairs, Kharkiv.

Biographies

Ruslan Orlovskyi received the specialist's degree in law from Yaroslav Mudryi National Law University in 1995, the PhD in law from Yaroslav

Mudryi National Law University in 2001, and the doctor of law degree from Yaroslav Mudryi National Law University in 2019. He works as the Professor at the Department of Criminal Law, Yaroslav Mudryi National Law University. The field of scientific interests includes complicity in a crime, organized crime, human trafficking, legalization of property obtained through criminal means, corruption. He has been a reviewer for many highly respected journals.

Sergiy Kharytonov received the specialist's degree in law from Yaroslav Mudryi National Law University in 1995, the PhD in law from Kharkiv National University of Internal Affairs in 2000, and the doctor of law degree from Yaroslav Mudryi National Law University in 2019. He works as Head of the Department of Criminal Law Policy, Yaroslav Mudryi National Law University. His research areas include criminal low, military crimes, cybercrime. He has been serving as a reviewer for many highly-respected journals.

Igor Samoshchenko received the specialist's degree in law from Yaroslav Mudryi National Law University in 1989, the PhD in law from Yaroslav Mudryi National Law University in 1997. He works as the Dean of the

Faculty of International Law, Yaroslav Mudryi National Law University. His research areas include criminal low, comparative criminal law, international criminal law. He completed internships and attended educational events with the support of the USAID New Justice Program and the OSCE Project Coordinator in Ukraine (2018–2019).

Olha Us received the specialist's degree in law from Yaroslav Mudryi National Law University in 2001, the PhD in law from Yaroslav Mudryi National Law University in 2005, and the doctor of law degree from Yaroslav Mudryi National Law University in 2021. She works as the Professor at the Department of Criminal Law, Yaroslav Mudryi National Law University. The field of scientific interests includes complicity in a crime, qualification of crimes, punishment, human trafficking, corruption. She has been a reviewer for many highly respected journals.

Volodymyr Iemelianenko received the specialist's degree in law from Yaroslav Mudryi National Law University in 2003, the PhD in law from Yaroslav Mudryi National Law University in 2009. He works as the Associate Professor of the Department of Criminal Law Policy, Yaroslav Mudryi National Law University. His research areas include criminal law, military crimes, transport crimes and cybercrimes. He has been serving as a reviewer for many highly-respected journals.