COMBATING CYBERCRIME AND CRIMINAL LEGAL MEASURES UNDER THE CONDITIONS OF THE STATE OF MARTIAL

[a] NATALIIA VESELOVSKA, [b]SERHII KRUSHYNSKYI,
[b]OLEH KRAVCHUK,
[c]OLEKSANDR PUNDA, [d]IVAN PISKUN

[a] *National Academy of Management, Ukraine*
[b] *Leonid Yuzkov Khmelnytskyi university of management and law, Ukraine*
[c]*Khmelnytskyi National University, Ukraine*
[d]*Ivan Cherniakhovski National Defence University of Ukraine, Ukraine*
email: [a]veselovska@ukr.net, [b]krusnynskyi.s@gmail.com,
[b] kravchuk@gmail.com, [c] punda.o@gmail.com,
[d] piskun.i@gmail.com

Abstract: The manuscript is devoted to the peculiarities of the application of criminal legal measures against cybercrimes under martial law. During the research, we found an opportunity to formulate the author's recommendations for solving the most complex problems of law enforcement, as well as to propose changes to the Criminal Code of Ukraine, aimed at eliminating the shortcomings of the analyzed Law, the adoption of which will contribute to the achievement of greater effectiveness of the relevant criminal law prescriptions.

Keywords: wartime, information, cybercrime, martial law, information and communication systems, unauthorized interference

1 Introduction

In the conditions of the military invasion of the Russian Federation in Ukraine, the issue of ensuring cyber security, primarily the directions of strengthening the state's defense capabilities in cyberspace and combating cybercrime, is becoming especially urgent. Cyber security strategy of Ukraine, approved by the decision of the National Security and Defense Council of Ukraine and put into effect by Decree of the President of Ukraine dated August 26, 2021 No. 447, the main threats to cyber security include cybercrime, which "damages information resources, social processes, individual citizens, reduces public trust in information technologies and leads to significant material losses" (paragraph 3). In order to strengthen the ability to combat cybercrime, it is planned to: complete the implementation of the provisions of the Convention on Cybercrime into the legislation of Ukraine; development of approaches to the implementation of state policy in the sphere of ensuring the rights of citizens cyberspace; regulation at the legislative level of the legal status of cryptocurrencies; introduction of the practice of conducting an information campaign regarding the actions of citizens in the event that they encounter cyber fraud and other cybercrimes, etc.

Increasing the ability to protect Ukraine against attacks in cyberspace is relevant in the context of the Russian invasion. Combating cybercrime is a form of repelling and deterring the aggression of the Kremlin regime against Ukraine. In the current conditions, cybercriminals have become more active in Ukraine. This caused significant material damage to state information portals, as well as critical infrastructure facilities. Society began to distrust information technologies. In addition, many Ukrainians are skeptical of digital services.

As for cybercrime, it is computer and network crime Moore R. (2010). A computer can be used as a means of committing a crime, or it can be a target Kruse W.G., Heiser J.G. (2002). Cybercrime can harm everyone's security and financial well-being Bossler, A.M. and Berenblum T. (2019). To combat cybercrime, it became necessary to create new structures in the police forces of all states. Even the European Cybercrime Center (EC or EC³) has been created, a body of the Police Office of the European Union (Europol) headquartered in The Hague, which coordinates cross-border law enforcement activities against computer crime and acts as a center of technical expertise on the matter. Accordingly, on October 5, 2015, the Cyber Police was established as a structural unit of the National Police. The main goal of the creation of the cyber police in Ukraine was the reform and development of the units of the Ministry of Internal Affairs of Ukraine, which ensured the training and functioning of highly qualified specialists of the expert-operational and investigative units of the Ministry of Internal Affairs, involved in combating cybercrime, and who are able to use the latest technologies in operational and service activities at a high professional level.

This topic has become the object of numerous studies by domestic scientists, such as: P. Bilenchuk, B. Kormych, T. Kostecka, E. Kravets, N. Lebedeva, V. Monakhov, V. Naumov, R. Shagieva.

Nowadays, cyber crimes are quite common. feel protected from such crimes is practically impossible. The boundaries of cyberspace are limitless, hackers have had enough developed skills to remain incognito in it and therefore it creates problems during investigation such crimes. Thousands of crimes every day are associated with the theft of personal data, funds from accounts, blocking activities. Under the circle of possible victims are not only people, but also companies and even state The concept of cyber security refers to the protection of the vital interests of societyand the state in the process of using cyberspace, which ensures the sustainable development of information society and digital communication environment.

2 The initial presuppositions

Russia's armed aggression had a negative impact on most aspects of the peaceful life of Ukrainians until February 24. Currently, the issue of researching the relationship between the interests of the individual and the state, which was considered in many scientific-legal and philosophical-methodological studies, is relevant. However, the legal nature of special issues regarding criminal-legal countermeasures in the conditions of martial law, which remained unexplored or insufficiently researched, is currently becoming very topical.

3 Methods

The methodological basis for writing this article was different methods of scientific knowledge were used. In particular, the method of comparison and analogy is used to study the legal regulation of various types of cybercrimes. The observation method was used to get acquainted with the essence of cybercrimes and the general specificity of this phenomenon. The method of generalization was used to study various types of cybercrimes. A systematic approach with dialectical, formal-logical and structural-functional methods and other general scientific methods of research, as well as special legal methods: comparative-legal and formal-legal, were also used.

4 Results and discussion

The concept of cybercrime is still unfamiliar to law enforcement agencies, but criminal actions in which cyberspace is used, carries a large social danger The transnational nature of criminally illegal activity using cyberspace provides reasons believe that the development of a general policy on the main issues has be part of any cybercrime strategy.

In Ukraine, every modern socially active person uses mobile devices and uses the Internet, government bodies switch to electronic document management, stable operation of the banking sector, railways and air transport, large enterprises depend on the stability of the cyberspace with which they work and are based on communication using electronic means connection During the development of new social relations, crime also arises. In the conditions of war, such a thief becomes a combat unit, and his main tool is cyber attacks and evil. Therefore, during martial law, attacks are possible not only from the enemy, who uses the information space to damage Ukraine's defense capabilities, but also from those who decided to take

advantage of the situation of overloaded law enforcement agencies and profit from it, the funds of our citizens. And as we can see, during the eighth month of the war, cybercrime in Ukraine is only growing steadily.

In the conditions of the Russian Federation's military invasion of Ukraine, the issue of ensuring cyber security, primarily in the areas of strengthening the state's defense capabilities in cyberspace and countering cybercrime, is gaining particular relevance Kravchuk O.V. (2016).

It is worth analyzing the opinion of foreign and domestic scientists regarding the definition of cybercrime. So O. Kopan provides a definition in the dictionary of cyber security terms cybercrime as illegal interference in the work of cybernetic systems, the main control link of which is a computer,creation and use for criminal purposes of a certain cybernetic system, use of existing ones for criminal purposes of cybernetic systems Manzhai O., Kuryliuk Y., Miroshnykov I. et al. (2022).

M.V. Kocharevsky correlates the concept of cybercrime and crime in the field of computer information and defines how one of the types of crimes in the field of information security, which provided by the Criminal Code of Ukraine, socially dangerous, guilty, committed the subject of the crime of actions that cause damage, provided by means of computer technology, to relations in the sphere of implementation of information needs Karchevsky N.V. (2016)

The legal basis for ensuring cyber security of Ukraine is the Constitution of Ukraine, the laws of Ukraine on the foundations of national security, the principles of internal and foreign policy, on electronic communications, on the protection of state information resources and information, the requirements for the protection of which are established by law, the Law of Ukraine "On the Fundamentals of Ensuring Cyber Security of Ukraine" and other laws of Ukraine, the Convention on Cybercrime, other international treaties, the binding consent of which was given by the Supreme Court. Council of Ukraine. Councils of Ukraine, decrees of the President of Ukraine, acts of the Cabinet of Ministers of Ukraine, as well as other normative legal acts adopted to implement the laws of Ukraine. According to Art. 1 of the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine", cyber security is the protection of the vital interests of a person and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace.

According to Art. 4 of the Law of Ukraine "On the Basics of Ensuring Cyber Security of Ukraine", the objects of cyber security are the constitutional rights and freedoms of a person and a citizen; society, sustainable development of information society and digital communication environment; the state, its constitutional system, sovereignty, territorial integrity and inviolability; national interests in all areas of human life, society and the state; objects of critical infrastructure, and objects of cyber protection include communication systems of all forms of ownership, in which national information resources are processed and/or which are used in the interests of state authorities, local governments, law enforcement agencies and military formations formed in accordance with the law; objects of critical information infrastructure; communication systems used to meet public needs and/or implement legal relations in the fields of electronic government, electronic public services, electronic commerce, and electronic document management. An important international legal act in the field of combating cybercrime is the Convention on Cybercrime dated November 23, 2001, ratified by the Law of Ukraine dated September 7, 2005 No. 2824-IV. In order to strengthen the fight against cybercrime and cyberattacks, the 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 investigation "on hot pursuit" has already been adopted. during the legal regime of martial law in Ukraine. Measures to Counter Cyber Attacks" dated March 15, 2022 No. 2137-IX and the Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Improving the Effectiveness of Countering Cybercrime in Martial Law" dated March 24, 2022 No. 2149-IX.

In turn, the Criminal Code of Ukraine contains something another classification of crimes in the field of computer information. In particular, section 16 criminal offenses in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks includes 6 types of crimes in the field of computer information:

Unauthorized interference with the operation of electronic computing machines (computers), automated systems, computer networks or telecommunication networks.

1. Creation for the purpose of use, distribution or sale of malicious software or technical means, as well as their distribution or sale.
2. Unauthorized sale or distribution of information with limited access, which is stored in electronic computing machines (computers), automated systems, computer networks or on media of such information.
3. Unauthorized actions with the information being processedin electronic computing machines (computers), automated systems, computer networks or stored on the media of such information, committed by a person who has the right access to it.
4. Violation of the rules of operation of electronic computing machines (computers), automated systems, computer networks or telecommunication networks or order or rules for the protection of the information processed in them.
5. Obstructing the work of electronic computers machines (computers), automated systems, computer networks or telecommunication networks by mass distribution of telecommunication messages. It is worth noting that the list of crimes in the field of computer information contained in the Criminal Code of Ukraine, does not cover the entire range of criminal acts committed in cyberspace.

The cyber security strategy of Ukraine, approved by the decision of the National Security and Defense Council of Ukraine and put into effect by the Decree of the President of Ukraine No. 447 dated August 26, 2021, includes cybercrime as the main threats to cyber security, which "damages information resources, social processes, individual citizens, reduces public trust in information technologies and leads to significant material losses" (paragraph 3). In order to strengthen the ability to combat cybercrime, it is planned to: complete the implementation of the provisions of the Convention on Cybercrime into the legislation of Ukraine; development of approaches to the implementation of state policy in the sphere of ensuring the rights of citizens in cyberspace; regulation at the legislative level of the legal status of cryptocurrencies; introduction of the practice of conducting an information campaign regarding the actions of citizens in the event that they encounter cyber fraud and other cybercrimes, etc.Since the beginning of the full-scale invasion and the introduction of martial law in Ukraine, the problem of compliance of the current criminal legislation of Ukraine with the latest challenges and threats related to the war turned out to be extremely urgent. That is why the Ukrainian parliament made a number of changes and additions to the Criminal Code of Ukraine (hereinafter - the Criminal Code) already under martial law. The Criminal Code was supplemented with new categories of crimes, in particular:

- Art. 111-1 "Collaborative activity";
- Art. 111-2 "Assistance to the aggressor state";
- Art. 114-2 "Unauthorized dissemination of information about the transfer, transfer of weapons, armaments and war supplies to Ukraine, the movement, transfer or placement of the Armed Forces of Ukraine or other military formations formed in accordance with the laws of Ukraine,

committed under conditions of war or a state of emergency";
- Art. 201-2 "Illegal use for profit of humanitarian aid, charitable donations or free aid";
- Art. 436-2 "Justification, recognition as legitimate, denial of the armed aggression of the Russian Federation against Ukraine, glorification of its participants." In addition, additions or changes were made to a number of articles of the Criminal Code, in particular, criminal liability was increased for the commission of certain offenses (theft - Article 185, robbery - Article 186, robbery - Article 187, extortion - Article 189, etc.).

Article has undergone far more serious changes. 361 of the Criminal Code, according to the updated version of which:

1) the very fact of unauthorized interference in the work of information (automated), electronic communication, information and communication systems, electronic communication networks is recognized as criminally illegal (for the sake of convenience, further on in this publication, the single phrase "unauthorized interference" will be used to denote the corresponding criminal offense) - regardless from whether such actions led to the leakage, loss, forgery, blocking of information, distortion of the information processing process or violation of the established order of its routing, the occurrence of which from now on should be considered not as constituting a crime (as before), but as a qualifying feature of the criminal offense under consideration (hereinafter - k. pr.) (new part 3 of article 361 of the Criminal Code).

From now on, for the qualification of actions according to this norm, it is enough for a person to commit an action in the form of unauthorized intervention, and the occurrence of harmful consequences (such as leakage, forgery, blocking of information, etc.) is not required. Thus, the legislator criminalized an act for which there was no criminal liability before. At the same time, this article provides that interference in the operation of information (automated), electronic communication, information communication systems, electronic communication networks is not considered unauthorized, if such interference is carried out in accordance with the Procedure for searching and identifying potential vulnerabilities of such systems or networks (part 6 of Article 361). In addition, sanctions for the commission of a criminal offense under Article 361-1 of the Criminal Code are being strengthened Iasechko S., Pereiaslavska S., Smahina O. Et al. (2022)

M. I. Havronyuk made a remark, assuming that excessive criminalization is taking place here, since, according to the scientist, unauthorized interference in the work of the specified systems or networks is not a crime in itself, since it does not create any consequences that could be subject to the action criminal liability. the concept of significant damage (Article 11 of the Criminal Code). For example, a situation is simulated when a work colleague wants to watch news on another employee's computer, and his own computer is under repair, turns it on and searches on sites (minor action) Kronivets T., Tymoshenko Y., Diachenko O. et al. (2021)

At the same time, we note that the question of the justification of the criminalization of the specified acts can only be resolved based on the results of a separate study, within the scope of which it would be:

a) a clearly defined social danger of unauthorized intervention, the "price" of which - encroachment on private life, taking into account the comprehensive digitalization of society, only increases every day;
b) relevant foreign experience is analyzed in detail.

Even without delving into the research of this issue, I would still like to draw attention to the fact that the parliamentarians of at least several European countries assess the public danger of unauthorized interference in the work of information systems in such a way that they recognize this act as criminally illegal - either unconditionally or on the condition , that these actions are accompanied by the overcoming (violation) of security measures - regardless of any of its consequences (see, for example: Article 118-a of the Criminal Code). of Austria, Article 217 of the Penitentiary Code of Estonia, Part 3 of Article 197 of the Criminal Code of Spain, Article 138 of the Criminal Code of the Netherlands, Article 267 of the Criminal Code of Poland, etc.); c) Ukraine's international obligations are taken into account. In particular, in Art. 2 of the Council of Europe Convention on Cybercrime (ratified by Ukraine in 2005) provides for the need to criminalize illegal access, that is, intentional access to the entire computer system or its part without the right to do so. Criminal liability in this case is not associated with any consequences.

At the same time, it should be taken into account that in the same norm it is indicated that the country can demand that such an offense was committed in violation of security measures for the purpose of obtaining computer data or for another dishonest purpose, or in connection with a computer system, connected to another computer system;

2) increased liability: – firstly, for the actions provided for in part 1 or part 2, which created the danger of serious man-made accidents or ecological catastrophes, death or mass illness of the population or other serious consequences (new part 4); - secondly, for the actions provided for in part 3 or part 4, committed during martial law (new part 5);

3) the actions provided for in parts 1-4 of this article are not considered unauthorized interference, if they were carried out in accordance with the procedure for searching and identifying potential vulnerabilities of such systems or networks (new part 6). Unfortunately, as in the situation with most other "military" changes to the Criminal Code, not all updates associated with the adoption of the Law of March 24, 2022 (including those mentioned above) should be evaluated positively Iasechko S., Kuryliuk Y., Nikiforenko V. et al. (2021).

All these changes are the state's reaction to the operational situation that developed during the war, so the vast majority of them concern either the criminalization of certain acts that did not exist before the war, or the strengthening of responsibility for some offenses. It should be noted separately the relevance of the problem of combating crime in cyberspace, since in the conditions of war in Ukraine, the number of illegal actions in the digital environment, which are carried out with the aim of manipulating and destabilizing the situation in the country, disruptions in the work of state institutions, theft of confidential data, damage to equipment, tasks, is increasing other damages Iasechko S., Ivanovska A., Gudz T., et al (2021).

Even taking into account the peculiarities of the development of each of the states, it is possible to offer the most general (universal) countermeasures against cybercrime, which will be effective in Ukraine as well. In the first in turn, this can be achieved by establishing criminal liability for crimes of the specified type, as well as the development of appropriate strategies for ensuring information security criminal legal means. It also seems appropriate, for the purpose of emphasis, to include at the level of national (including Ukrainian) and international criminal legislation, a norm that determined one of the tasks of the criminal law to ensure the protection of information security; it is expedient to conduct separate studies and develop recommendations for the training of professionals in legal sphere, ensuring legality in their activities within the limits of current informational needs society at the national level.

5 Conclusion

To specify the essence of the investigated type of crime, there is a need to develop its criminological classification. It will be useful both for scientists in order to further improve forensic methods, and for practitioners in order to properly organize the process of investigating cybercrimes, which will not allow persons involved in cybercrimes to avoid criminal liability.

Currently, cybercrimes are the most progressive types of criminal offenses that have covered almost all spheres of human life, the state as a whole and individual citizens are harmed by cybercriminals. It is worth noting that due to the complex and specific nature of cybercrimes, there is no universal model for identifying all possible categories of threats and directly investigating the specified type of criminal offenses. Analyzing the doctrinal definitions of the concept of cybercrime offered by both domestic and foreign scientists, we can come to the conclusion that currently there is no clear concept of cybercrime that would characterize it through its main features unique to it.

Cybercrime in wartime is generally on the rise, as since the start of the full-scale invasion of Russia, the battles have not only been fought on the home front, but also on the cyber front, where government websites, broadcasters' websites, media outlets, and critical infrastructure enterprises have been subject to periodic cyberattacks, so we consider the above proposals regarding the improvement of criminal legislation to be relevant and necessary not only during martial law, but also in post. - the war period.

Literature:

1. Moore, R. (2010) Cyber crime: Investigating High-Technology Computer Crime. Routledge. 312 p
2. Iasechko S., Ivanovska A., Gudz T., et al (2021). *Information as An Object of Legal Regulation in Ukraine*/ IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.5, pp. 237-242 https://doi.org/10.22937/IJCSNS.2021.21.5.33
3. Iasechko S., Kuryliuk Y., Nikiforenko V., et al (2021). *Features of Administrative Liability for Offenses in the Informational Sphere*/ IJCSNS International Journal of Computer Science and Network Security, Vol. 21 No. 8 pp. 51-54 https://doi.org/10.22937/IJCSNS.2021.21.8.7
4. Kruse W.G., Heiser J.G. (2002) Cjpputer forensics: incident response essentials. . Addison-Wesley. p. 392
5. Bossler, A.M., Berenblum T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice. 20 October 2019 42 (5): 495-499.
6. Cyber Police of Ukraine National Police of Ukraine. Site URL: https://cyberpolice.gov.ua/ (date of application: 09/15/2022).
7. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
8. Convention on cybercrime dated November 23, 2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
9. On amendments to the Criminal Code of Ukraine to increase the effectiveness of the fight against cybercrime under martial law: Law of Ukraine dated March 24, 2022 No. 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text
10. Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Increasing the Effectiveness of Combating Cybercrime in the Conditions of Martial Law"
11. Scientific and practical commentary on the Criminal Code of Ukraine / edited by M. I. Melnyk, M. I. Havronyuk. 10th ed., revised. and added Kyiv: VD "Dakor", 2018. 1360 p
12. Over 100 days of war: how Ukraine resisted attacks on the cyber front // ESET. June 07, 2022.
13. Manzhai O., Kuryliuk Y., Miroshnykov I. et al. (2022). Criminal and Legal Protection of Information Relations. International Journal of Computer Science and Network Security. Vol. 22. No. 5. pp. 284–288.
14. Kalinina A. (2021). Influence of the quarantine within the prevention of COVID-19 on the migrants' crime in Ukraine. Migration & Law. Vol. 1. Issue 1. pp. 24–41.
15. Iasechko S., Pereiaslavska S., Smahina O. Et al. (2022) Artificial Intelligence In The Modern Educational Space: Problems And Prospects IJCSNS International Journal of Computer Science and Network Security. Vol. 22 No. 6, pp. 25-32.
16. Kravchuk O.V. (2016) Cybersecurity in hybrid warfare: a study guide. Khmelnytskyi: Hmm. TsNTEI, 218 p.
17. Karchevsky N.V. (2016) Cybercrime or crime in the sphere the use of information technologies. Cybersecurity in Ukraine: legal and organizational issues: materials all-Ukrainian. Science and practice conference, Odesa, October 21, pp. 10–15.

Primary Paper Section: A

Secondary Paper Section: AG