Criminal and Legal Countermeasures against Cybercrime in the Conditions of Martial Law

Nataliia Veselovska[†], Serhii Krushynskyi[††], Oleh Kravchuk[††], Oleksandr Punda[†††], Ivan Piskun[††††]

[†]National Academy of Management, Ukraine
[††]Leonid Yuzkov Khmelnytskyi university of management and law, Ukraine
[†††]Khmelnytskyi National University, Ukraine
[††††]Ivan Cherniakhovski National Defence University of Ukraine, Ukraine

Summary
The article is devoted to the consideration of the features of the application of criminal and legal countermeasures against cybercrime in the conditions of martial law. While conducting this research, we found an opportunity to formulate the author's recommendations for solving the most complex law enforcement problems, as well as to propose changes to the Criminal Code of Ukraine aimed at eliminating the flaws of the analyzed Law, the adoption of which will contribute to the achievement of higher efficiency of the relevant criminal law prescriptions. It is argued that the removal of the previously existing in the footnote of Art. 361 of the Criminal Code of a fundamentally important caveat regarding the fact that when assessing "significant damage", the mentioned property equivalent was to be taken into account only when such damage consisted in causing material damage, which led to a significant and unjustified narrowing of the scope of potential application of Part 4 of Article 361 of the Criminal Code.

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

1. Introduction

The issue of increasing the ability to protect Ukraine against attacks in cyberspace is urgent in the context of the Russian invasion. Combating cybercrime is a form of repelling and deterring the aggression of the Kremlin regime against Ukraine. Recently, cybercriminals have become more active in Ukraine. This caused significant material damage to state information portals, as well as critical infrastructure facilities. As a result, society began to mistrust information technologies. In addition, many Ukrainians are skeptical about digital services.

Cybercrime is computer and network related crime [1]. A computer can be used as a means of committing a crime or it can be a target [2]. Cybercrime can wreak havoc on everyone's security and financial well-being [3]. In order to combat cybercrimes, it became necessary to create new structures in the police forces of all states. Even the European Cybercrime Center (EC or EC³) was created - a body of the Police Office of the European Union (Europol) with headquarters in The Hague, which coordinates cross-border law enforcement activities against computer crime and acts as a technical expertise center for this question. Accordingly, on October 5, 2015, the Cyber Police was created as a structural unit of the National Police [4]. The purpose of creating the Cyber Police in Ukraine was to reform and develop the units of the Ministry of Internal Affairs of Ukraine, which ensured the training and functioning of highly qualified specialists in expert, operational and investigative units of the police, involved in countering cybercrime, and capable of using the latest technologies in operational and service activities at a high professional level.

The main tasks of the cyber police include:
- implementation of state policy in the field of combating cybercrime;
- informing the population in advance about the emergence of the latest cybercrimes;
- implementation of software tools for systematization and analysis of information about cyber incidents, cyber threats and cyber crimes;
- responding to requests from foreign partners received through the channels of the National round-the-clock network of contact points;

Manuscript received December 5, 2022
Manuscript revised December 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.12.11

- participation in improving the qualifications of police officers regarding the use of computer technologies in combating crime;
- participation in international operations and cooperation in real time, ensuring the operation of a network of contact points between 90 countries of the world;
- combating cybercrimes in the field of using payment systems [4].

2. Theoretical Consideration

Every modern socially active person in Ukraine uses mobile devices and uses the Internet, government bodies are switching to electronic document management, the stable operation of the banking sector, railways and air transport, large enterprises depends on the stability of the cyberspace with which they work, and is based on communication using electronic means connection

Where new social relations develop, crime also appears. According to the official statistics of the Office of the Prosecutor General of Ukraine, in the last 8 years alone, the number of detected cybercrimes has increased almost 7.5 times (and this does not take into account classic crimes involving the use of computer technology, as well as the level of latency of such crime).

In the conditions of war, such a thief becomes a combat unit, and his main tool is cyber attacks and hacking. In addition, during the martial law, attacks are possible not only from the enemy who uses the information space to harm Ukraine's defense capabilities, but also from those who have decided to take advantage of the situation when law enforcement agencies are overburdened and profit from 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 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 [19].

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 external policy, electronic communications, the protection of state information resources and information, the requirement for the protection of which is established by law, the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" and other laws of Ukraine, the Convention on Cybercrime, other international treaties, the binding consent of which has been given by the Verkhovna Rada 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 the national security of Ukraine in cyberspace.

According to Art. 4 of the Law of Ukraine "On the Basic Principles 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 spheres of life of a person, 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 self-government bodies, 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, electronic document management [5]. 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 [6]. 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" was adopted already during the legal regime of martial law in Ukraine. Countermeasures against Cyber Attacks" dated March 15, 2022 No. 2137-IX [8] and the Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Improving the Effectiveness of Combating Cybercrime in the Conditions of Martial Law" dated March 24, 2022 No. 2149-IX [7].

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 [1] (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.) [8].

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 [9-10].

Regarding the relevant changes, M. I. Havronyuk made comments, suggesting that excessive criminalization is taking place here, because, according to the scientist, unauthorized interference in the work of the mentioned systems or networks is not a crime in itself, since does not create any consequences that could be covered by the concept of significant damage (Article 11 of the Criminal Code). At the same time, as an example, a situation is simulated when a work colleague wants to watch the news using another employee's PC, while his own is being repaired, turns it on and searches the sites (minor act) [11]. With the arguments of the scientist, at the same time, I note that, in my opinion, the question of the justification of the criminalization of the mentioned acts can be resolved only based on the results of a separate study, within the limits of which it would be:

a) clearly defined the social danger of unauthorized intervention, the "price" of which is an encroachment on the privacy of life, taking into account the comprehensive digitalization of society, only grows every day;

b) relevant foreign experience is analyzed in detail.

In particular, without even delving into the study 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 Criminal Code of the Netherlands, Article 267 of the Criminal Code of Poland, etc.); c) the international obligations of Ukraine are taken into account. In particular, in Art. 2 of the Council of Europe Convention on Cybercrime (ratified by Ukraine in 2005) stipulates the need to criminalize illegal access, that is, intentional access to an 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 may require that such an offense be committed by violating security measures for the purpose of obtaining computer data or with another dishonest purpose, or in relation to a computer system connected with another computer system;

2) increased liability: – firstly, for the actions provided for in part 1 or part 2, which created the danger of severe technological accidents or ecological disasters, 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 now 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 related to the adoption of the Law of March 24, 2022 (including those mentioned above) should be evaluated positively [14-15].

So, 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 take place before the war, or the strengthening of responsibility for some offenses. Separately, it is necessary to mention the relevance of the problem of combating crimes in cyberspace, since in the conditions of war in Ukraine, the number of illegal acts in the digital environment, which are carried out with the aim of manipulation and destabilization of the situation in the country, disruptions in the work of state institutions, theft of confidential data, damage to equipment, tasks other damage [16-18]. Therefore, it is clear that in order to damage Ukraine's defense capabilities, Russia actively uses virtual space to carry out cyber attacks, spread fakes, recruit the population, including children, etc. Specialists of the international company ESET, which specializes in the development of antivirus software, investigated the prevalence of cyber threats for January-September 2022 and found that during this period the total number of detected threat samples increased by 20% compared to the last four months of 2021 [12].

It should also be noted that the theme of the war in Ukraine is actively used by cyber fraudsters in their schemes around the world, who, under the guise of fake charities, lure donations to support Ukraine. On average, ESET telemetry detected 4.8 million web threats and 370,000 malicious URLs worldwide every day. At the same time, the number of blocked phishing URLs increased by almost 30% [13].

Conclusions

Therefore, in order 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 with the aim of further improving forensic methods, and for practitioners with the aim of properly organizing the process of investigating cybercrimes, which will not allow persons involved in cybercrimes to avoid criminal responsibility.

Crime in the digital environment during the war generally increases, because since the beginning of the full-scale invasion of Russia, battles were fought not only on the front, but also on the cyber front, where government websites, broadcasters' websites, media and critical infrastructure enterprises are periodically subjected to cyber attacks. On the other hand, 214 the topic of war is actively used by cyber fraudsters and not only in Ukraine, therefore we consider the above proposals regarding the improvement of criminal legislation to be relevant and necessary not only during martial law, but also in the post-war period.
Obviously, these issues require further careful study. Nevertheless, attempts to improve the legal mechanism for ensuring information security in Ukraine deserve a positive assessment.

References

[1] Moore, R. (2010) Cyber crime: Investigating High-Technology Computer Crime. Routledge. 312 p
[2] Kruse W.G., Heiser J.G.(2002) Cjpputer forensics: incident response essentials. . Addison-Wesley. p. 392
[3] Bossler, A.M., Berenblum T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice. 20 October 2019 42 (5): 495-499.

[4] Cyber Police of Ukraine National Police of Ukraine. Site URL: https://cyberpolice.gov.ua/ (date of application: 09/15/2022).
[5] 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
[6] Convention on cybercrime dated November 23, 2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
[7] 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
[8] Criminal Code of Ukraine dated April 5, 2001 No. 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
[9] Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Increasing the Effectiveness of Combating Cybercrime in the Conditions of Martial Law"
[14] 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.
No. 2149-IX dated March 24, 2022.
URL: https://zakon.rada.gov. ua/laws/show/2149-20#Text
[10] The Council strengthened the capabilities of the national cyber security system / Ukrinform from March 24, 2022.
URL: https://cutt.ly/rXgAz1M
[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.
URL: https://cutt.ly/fXgAwM6
[13] Boyko I.(2022) Rating of Internet threats: IT experts analyzed the impact of the war in Ukraine on cyber security / UNIAN Information Agency, June 4, 2022.
URL: https://cutt.ly/sXgAfmj
[15] 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.
[16] Kronivets T., Tymoshenko Y., Diachenko O. et al. (2021) Artificial intelligence as a key element of digital education / IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.10б pp. 67-72 https://doi.org/10.22937/IJCSNS.2021.21.10.9
[17] 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.
[18] Iasechko S., Kuryliuk Y., Nikiforenko V. et al. (2021). Features of Administrative Liability for Offenses in the Informational Sphere. International Journal of Computer Science and Network Security. Vol. 21. No.8. pp. 51–54.
[19] Kravchuk O.V. (2016) Cybersecurity in hybrid warfare: a study guide. Khmelnytskyi: Hmm. TsNTEI, 218 p.