TYPES OF CYBER CONFLICTS AND THE ROLE OF THE STATE IN THEIR PREVENTION AND SOLUTION

Iryna Sopilko

Doctor of Juridical Sciences, Professor, Honored Lawyer of Ukraine,
Academician of the Academy of Sciences of the Higher School of Ukraine,
Dean of the Faculty of Law of National Aviation University of Kyiv (Kyiv, Ukraine),
E-mail: sopilko_i@ukr.net,
ORCID ID: 0000-0002-9594-9280

Viktoriya Cherevatiuk

PhD in History, Associate Professor, Associate Professor of Theory and History
of State and Law Department, Faculty of Law, National Aviation University of Kyiv (Kyiv, Ukraine),
E-mail: vitacherev@ukr.net,
ORCID ID: 0000-0002-4077-206X

SUMMARY. *The world of digital technologies, in which we learn to live, requires from us new qualitative knowledge and systematization of already existing ones. Undoubtedly, this is not only a new logical stage in the development of the technological sphere of mankind, but also the entire existing legal and political reality. At this stage, it is important to form the necessary definitions and definitions. Therefore, the study of types of cyber-conflicts, the role of the state in their prevention and resolution is relevant, and the problems of regulation and regulation of activities in cyberspace have long been key in the policy of many countries. The aim of the article is to clarify the concept of cyber conflict, types of cyber-conflicts and the role of the state in their prevention and resolution. Research methods: the use of general scientific and special legal methods of scientific knowledge, including dialectical, axiological, systemic and structural, generalization, comparative, allowed to clarify the essence of the concept of cyber conflict, its types and methods of prevention and resolution. Results: As a result of scientific research the qualitative features of cyber-conflicts, their types are revealed, the basic directions of research on this subject are outlined and the ways of the prevention and ways of the decision of such kind of conflicts are offered. The study allowed us to draw the following conclusions: the responsibility for the occurrence and spread of cyber-conflicts should be borne not only by the state, but also by each of us, because we worry about whether our data leaked into the network, we forget to behave properly so that data does not leak from our gadget. A systematic approach to the formation of the conceptual and terminological apparatus of cybersecurity should be applied, which will ensure adequate content of its content in accordance with the requirements for legal terminology, as well as enable harmonization with the terminology of current Ukrainian legislation and international acts. Today there is an urgent need to conceptually understand the new cybersecurity reality and to solve purely practical issues of streamlining the internal regulatory framework, the areas of responsibility of agencies involved in ensuring the cybersecurity of the state.*

Key words: *cyber, cyber-conflict, cyberspace, cyberwarfare, information society, cybervandalism; cyberespionage, Internet-crimes; cybercrime, cyberterrorism, cybersecurity.*

INTRODUCTION

Today, it is impossible to list all the possible security challenges. This is a pandemic, and rapid population growth, and environmental disasters, and water scarcity, and migration problems. In fact, there are many security threats, but our article will focus on cybersecurity and cyber conflicts, issues that are increasingly appearing in the press, in think tanks, in government reports, research, and so on. This is due to the fact that every day more and more Ukrainians gain access to the Internet using a telephone or computer, use e-mail, start running their own page on social networks, and e.t.c. With the help of the Internet we communicate, work, study, buy goods and services, carry out various banking operations, search for information. Therefore, it is natural that the number of conflicts closely related to information technology, including cyber-conflicts, is increasing. The structure of these conflicts does not change, only their subject and object acquire new features. Analyzing how state and local authorities are increasingly moving into the digital space today, we note the fact that they are increasingly becoming the subject of conflicts related to information technology. The development of the information society encourages state and local authorities to create and maintain a website, e-mail,

implement their services via the Internet, electronic document management system and more. It should also be noted that with the rapid development of information technology, there are those who want to make money on it, but make money through illegal actions and technologies. Therefore, we can safely predict that the number of conflicts in the field of information technology, including cyber-conflicts, will only grow rapidly. And the state must make every effort to prevent and resolve such conflicts. That is why, as Filinovych V.V. notes, the problem of responsibility of Ukrainian state bodies and Ukraine itself for violating the rights of its citizens in the field of cyber conflicts, in particular cybercrimes, should be regulated in more details at the legislative level. This should happen through the involvement of both public authorities and the private sector of the Ukrainian economy [1, p. 148].

The aim of the study is to clarify the concept, types of cyber-conflicts and the role of the state in their prevention and resolution.

REVIEW OF THE LITERATURE

Among domestic researches of normative-legal problems of cybersecurity the works of M. Ozhevan, O. Dzioban, V. Pylypchuk, V. Petrov deserve special attention. The conceptual framework for the study of cyberspace problems in the geopolitical sense is created by the study of the information society and its derivatives. In addition to the "classical" works of E. Toffler, F. Makhlup, F. Fukuyama, Y. Hayashi, M. Bangemann, M. McLuhan, G. Reinhold, the works of I.M. Sopilko, V.A. Lipkan, M. Ozhevan, I. Pedak, Y. Pavlenko, I. Danilin, .Dubov, R. Barbrook, D. Cameron, F. Millrach, M. Kapoor, N. Gingrich, J. Naya Jr., T. Waden, J. Suorant, S. Zizek, A. Crocker, A. Weinstein, V. Skalatsky and others.

RESULTS

The problems of regulating and standardizing activities in cyberspace have long been key in the policies of many countries around the world. All of them are unequivocal in the statement that cyberspace is an international space, and the activities of states in cyberspace must first and foremost comply with international law. We agree with the opinion of Razmetaeva Yu.S., who believes that an individual state will not be able to resist possible cyber threats if it relies only on its own developments and excludes, for security reasons, some aspects of information exchange with others [2]. It should also be noted that the doctrines of national cybersecurity do not always have time to change as quickly as technology. Therefore, the combination of national and international cyber-defense strategies, dynamism is the way that leads to the security of cyberspace, including the prevention of conflicts in the information sphere. One can fully agree with the thesis that "both the protection of hardware and the protection of software are the main tasks of cybersecurity. However, both types of protection must be implemented and incorporated into national and international strategy (regulation) in order to achieve their goals "[3, p. 22].

Ukraine, integrated into the global digital space, as noted by D.V. Dubov, is exposed to various threats and negative impacts associated with the development of cyberspace (including the effects of rivalry between the US, Russia and China), which sharply raises cybersecurity issues at the national level. Therefore, there is a need to conceptually understand the new security (cybersecurity) reality and address purely practical issues of streamlining the internal regulatory field, areas of responsibility of agencies involved in cybersecurity, in general, the whole range of issues related to building an effective national cybersecurity system [4, p.11].

Regarding regulatory and legal support, there are different types of cybernorms, which are already regulated at one level or another in the legislation of different states.

J. Kenneth believes that among them are the following:

1) those that call for compliance with existing international legal norms concerning the responsibility of the state in the implementation of armed conflicts;

2) those that exclude the possibility of complete destruction or decommissioning of the Internet around the world;

3) norms of national law that oblige any state to assist another state that has been the victim of a cyberattack;

4) norms regulating the use of cyber-technologies in order to eliminate or prevent malicious actions [5].

It can be stated that none of the pre-existing categories singles out cyber conflict as a threat to the existence of cyberspace and cybersecurity, and, therefore, it is not settled. Note also that hidden or overt cyber conflicts have the greatest impact on the development of international relations.

If we talk about the concept of cyber-conflict, the most common and most acceptable is the following definition: cyber-conflict is a clash or confrontation of political actors in cyberspace, due to the conflict of their interests, values and views, which is carried out by technical means (IT) and psychological methods (through propaganda, manipulation, etc.). As for the structure, the subjects of cyber conflict will be able to be all participants in international relations who are able to defend their own interests and have the necessary tools (technologies).

Victor Gvozd divides them into several main groups, which include:

- the most powerful countries at the world level, namely the United States and China. In fact, they are the main players in the field of cyber confrontation;
- regional leaders, including the EU in the European region, Russia in Eurasia, India in Southeast Asia, Brazil in Latin America and South Africa in Africa;
- other countries in the world that pursue their interests through cyberspace, but only at the local

level and without the widespread use of subversive forms of action. Ukraine belongs to this group;

• pariah countries and various extremist and terrorist organizations that use cyberspace to carry out subversive activities against other countries and international organizations, including the world's leading states [6].

Experts also single out the spaces in which cyber-conflict occurs simultaneously: technical (technology-based tools) and psychological (people-based techniques). The technical space includes:

1) nature of access: wired or wireless; physical proximity or distance to the media of the required information;

2) the vulnerability of a system; its insecurity or defect;

3) the possibility of uncontrolled management of the required information after entering the desired system; can occur remotely [8, p.515].

And the psychological space of influence includes:

1) informational and psychological pressure on the enemy;

2) the destructive nature of the changing information;

3) propaganda, manipulation and dissemination of false information [5].

Examples of cyber-conflicts are: a coordinated hacker attack on the computer systems of Estonian government agencies in April 2007, an attack on the computer systems of Georgian government agencies during the armed conflict in South Ossetia in 2008, cyber attacks on Ukrainian energy companies in December 2015 , US cyberattacks on IS in April 2016, etc. You can also mention the Petya virus, which attacked on June 27, 2017. In five days, the attack caused damage of about $ 10 billion not only to Ukraine but also to other countries. Compared to last year, the number of cyberattacks and anomalies in Ukraine has doubled or tripled. More than 90% of all attacks coming from abroad are related to Russia and hacker groups funded by the Russian government [7].

The first thing that the state should take care of in order to resolve and prevent conflicts is to improve the organizational and legal norms of international cooperation in the fight against cybercrime and cyberterrorism.

According to O.R. Peleshchak, the current Ukrainian legislation is not ready to respond to modern cyber-threats, so a systematic approach should be applied to the formation of the conceptual and terminological apparatus of cybersecurity, which will ensure adequate content in accordance with the requirements of legal terminology, as well as will allow coordination with the terminology of the current Ukrainian legislation and international acts [9, p.301]. With the entry into force of the Decree of the President of Ukraine "Cyber Security Strategy of Ukraine. Safe cyberspace is the key to successful development of the country "- the general logic of rule-making activities to some extent took into account the logic of the content of the conceptual apparatus of cybersecurity, and also partially formulated a vision of new geopolitical conditions of the state and its role in global and national cyberspace [10]. The strategy is based on the provisions of the Constitution of Ukraine, laws of Ukraine "On National Security of Ukraine" and "On Basic Principles of Cyber Security of Ukraine", Convention on Protection of Human Rights and Fundamental Freedoms, Convention on Cybercrime, National Security Strategy of Ukraine approved by Presidential Decree of 14 September 2020 № 392, the Concept of Combating Terrorism in Ukraine, approved by the Decree of the President of Ukraine of March 5, 2019 № 53, other regulations.

Regarding the types of cyberconflicts, in our article we would like to draw attention to the most common of them, in particular:

- cyber vandalism;
- cyber espionage or computer espionage;
- Internet - crimes;
- cyberterrorism, etc.

Latysh K.V. believes that cyber vandalism as a form of vandalism is due to the following factors:

1. Uncontrollability, chaos and impunity, which became possible as a result of the application of the principles enshrined in the Declaration of Independence of Cyberspace, created by John Perry Burlow. It is this proposed unlimited freedom that has led to the spread of vandalism, which has moved from the real to the virtual.

2. Weak control, or inadequate protection of computer programs, website or other object of criminal encroachment, as a result of which such object is very vulnerable.

3. The moment of committing cyber-vandalism is chosen so that it is not available for external observation, but the consequences of such actions are available for viewing by the general public [11, p.118]

Cyber espionage or computer espionage is a term that refers to the unauthorized acquisition of information in order to gain personal, economic, political or military advantage, carried out using the bypass (hacking) of computer security systems, using malicious software. Cyber espionage is a cyberattack organized and sponsored by other governments that involves the theft of sensitive information for political, economic, or military purposes. Features of such cyberattacks are their duration, complexity and hidden nature, which complicates their prevention, detection and neutralization. Cyber espionage can be carried out both remotely, via the Internet, and by intrusion into computers and computer networks of enterprises by ordinary spies ("moles"), as well as hackers. Cyber espionage - espionage carried out in cyberspace or with its use [12].

There is no unified definition of this phenomenon at the national and international level. Therefore, I. Diorditsa proposes to include in the definition the following: criminal activity carried out by secret investigation, search for collection, theft and transfer

of information constituting a state secret, a foreign state, foreign organizations and their foreign representatives, if these actions are committed by a foreigner or a person statelessness using cybernetics methods. The object of this cyber-conflict is the external security of the state, its sovereignty, territorial integrity, state economic information security, cyberspace in general [13]. The parties to this conflict are the state, foreign nationals and stateless persons who have reached the age of 16.

Cybercrime - (computer crime) - a socially dangerous criminal act in cyberspace and / or with its use, liability for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine [12].

The term "cybercrime" is often used along with the term "computer crime", and often these terms are used interchangeably. Indeed, these terms are very close to each other, but still not synonymous. The concept of "cybercrime" (in English - cybercrime) is broader than "computer crime" (computer crime), and more accurately reflects the nature of such a phenomenon as crime in the information space. Thus, the Oxford Explanatory Dictionary defines the prefix "cyber -" as a component of a complex word. Its importance - relating to information technology, the Internet, virtual reality. The Cambridge Dictionary gives almost the same definition. Thus, "cybercrime" is a crime connected both with use of computers, and with use of information technologies and global networks. At the same time, the term "computer crime" mainly refers to crimes committed against computers or computer data [14].

Legislation regulates some aspects of cybercrime. In 2021, the Cyber Security Strategy of Ukraine was adopted, which aims to create a national cybersecurity system, the creation of the National Coordination Center for Cybersecurity. In October 2017, the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" was adopted, which defines the legal and organizational principles of protection of vital interests of man and citizen, society and state, national interests of Ukraine in cyberspace, main goals, directions and principles of state policy in the field of cybersecurity, the powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this area, the basic principles of coordination of their activities to ensure cybersecurity.

In addition to this Law, the legislation of Ukraine on cybersecurity also includes: the Constitution of Ukraine, the Criminal Code of Ukraine, the laws of Ukraine "On Information", "On Fundamentals of National Security", "On Information Protection in Information and Telecommunication Systems" and others.

The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" establishes a number of important definitions of terms, in particular: cybercrime, cybercrime and cyberspace. Cybercrime (computer crime) - a socially dangerous criminal act in cyberspace and / or with its use, liability for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine. Cybercrime - a set of cybercrimes. Cyberspace is an environment (virtual space) that provides opportunities for communication and / or implementation of public relations, formed as a result of the operation of compatible (connected) communication systems and the provision of electronic communications using the Internet and / or other global data networks.

In the Criminal code of Ukraine these crimes are fixed in section. 16 "Criminal offenses in the field of use of electronic computers (computers), systems and computer networks and telecommunications networks" and are represented by the following rules:

Art. 361 - unauthorized interference in the work of electronic computers (computers), automated systems, computer networks or telecommunication networks;

Art. 361-1 - creation for the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale;

Art. 361-2 - unauthorized sale or distribution of information with limited access, which is stored in computers (computer), automated systems, computer networks or on media of such information;

Art. 362 - unauthorized actions with information that is processed in electronic computers (computers), automated systems, computer networks or stored on the media of such information, committed by a person who has the right to access it;

Art. 363 - violation of the rules of operation of electronic computers (computers), automated systems, computer networks or telecommunication networks or the order or rules of protection of information processed in them;

Art. 363-1 - interference with the work of electronic computers (computers), automated systems, computer networks or telecommunication networks by mass distribution of telecommunication messages [15].

- Law of Ukraine of September 7, 2005 "On Ratification of the Convention on Cybercrime"
- Law of Ukraine of October 6, 2004 "On Amendments to the Law of Ukraine" On Payment Systems and Money Transfer in Ukraine "
- Law of Ukraine of December 23, 2004 "On Amendments to the Criminal and Criminal Procedure Codes of Ukraine" (on Liability for Computer Crimes)
- Law of Ukraine of May 31, 2005 "On Amendments to the Law of Ukraine" On Protection of Information in Automated Systems "

• Decree №32 / 2017 "On the decision of the National Security and Defense Council of Ukraine of 29.12.2016" On threats to cybersecurity of the state and urgent measures to neutralize them "

Also in the Convention on Cybercrime, which entered into force on 01.07.2006, the classification of cybercrime is presented. All of them are characterized by the presence of intention as an element of the

subjective side. In total - three categories of cybercrime:

1. crimes against the confidentiality, integrity and efficiency of computer data and systems - illegal access, illegal interception, interference with data exchange, interference with the operation of systems, improper use of hardware devices

2. computer crimes - falsification and forgery committed with the use of computer technology

3. crimes related to content - the production, distribution and storage of child pornography

Any Internet user can be the target of cybercrime.

Consider the most common types of cybercrime. One of them is online fraud - the seizure of funds from citizens through online auctions, online stores, websites and telecommunications [16]. Consider typical examples. Cybercriminals can be very resourceful when it comes to extorting money from Internet users. Attackers can use a variety of methods to attack their victims, from disguising themselves as government officials to creating fraudulent websites on the Internet, adapting them to current topics. Last year, many fraudsters, using the theme of the COVID-19 pandemic, pretended to be health authorities or offered to sell scarce goods for protection. Today, fraudsters are trying to make money by using users' interest in the topic of coronavirus drugs. Keep in mind that malicious schemes are not limited to health emergencies or global events. Therefore, there is a need to be careful when working on the Internet and check the available information, which will help to identify any schemes of attackers in a timely manner.

Phishing is a set of methods to extort logins and passwords, credit card numbers and other confidential information from Internet users [16]. Most often, attackers impersonate representatives of well-known organizations in emails or phone calls. Email phishing is one of the most common types of phishing, it uses the technique of "spray and pray", thanks to which hackers pretend to be a legitimate person or organization, sending mass e-mails to all e-mail addresses. Their purpose is to urgently cause reckless actions from you, for example, to click on a malicious link.

Vishing is a type of cybercrime in which the messages contain a request to call a certain city number, and during the conversation the confidential data of the cardholder are requested [16]. Popular vishing schemes include masking criminals for technical support. Victims are allegedly called on behalf of their provider or a well-known software or hardware vendor. Scammers claim to have detected a non-existent problem with your computer and then demand payment to fix it, sometimes downloading malicious software in the process.

Carding - illegal financial transactions using a payment card or its details, which are not initiated or confirmed by its holder [16]. The criminals find the details of payment cards on the broken servers of online stores, payment and payment systems, as well as personal computers (either directly or through remote access programs, "Trojans", "bots").

Cash trapping - theft of cash from an ATM by installing a special retaining pad on the ATM tent [16]. At the time of issuance of banknotes, the ATM raises the protective metal "curtain" and pushes out the money. However, if the ATM is equipped with criminal equipment (tape with scotch tape), the banknotes are glued to the tape, and the fraudulent bar does not "release" them from the ATM. Adequate and rapid response of banks to the danger - the installation of anti-caching pads used by the largest banks in Ukraine, a large-scale information campaign against ATM fraud, have led to a significant reduction in this type of crime.

Piracy is the illegal distribution of intellectual property on the Internet [16]. The essence of Internet piracy is the reproduction and distribution on the Internet of films, musical works, computer programs, other intellectual property, without the permission of the author or another person who has copyright and / or related rights, or without payment of remuneration for use works in the manner prescribed by law. In the legislation of Ukraine, the definition of Internet piracy is given in the Law of Ukraine "On Copyright and Related Rights": in Art. 50 Infringement of copyright and related rights in paragraph b) states that Internet piracy is the commission of any action that is recognized as a violation of copyright and (or) related rights using the Internet [17]. Internet piracy is global in nature, it cannot be defeated in a single country. But the world community and each country is trying to develop an effective mechanism for simplified and accelerated copyright protection on the Internet. Such legislative acts and draft laws as this are aimed at: the Law of Ukraine "On State Support of Cinematography in Ukraine" (1601-VIII) on March 23, 2017 - entered into force on April 26, 2017 [18]; EU Directive "On e-commerce" № 2000/31 / EC of 08.06.2000 [19]; EU Directive "On Copyright in the Digital Single Market" № 2019/790 / EU of 17.04.2019 [20].

Card sharing - providing illegal access to satellite and cable TV.

Pharming is about redirecting the victim to a false IP address. A scammer installs malware on computers that, when run on a computer, redirects the victim to fake sites instead of the sites they are looking for.

Reverse social engineering can only be carried out if the scammer is previously acquainted with the victim and deserves her trust. In this case, the victim turns to the scammer (for example, the system administrator), asking for help to recover the lost file (which was hidden by the scammer himself). At the same time, she is informed that such an action can be done as soon as possible only by logging into her account. Thus, the victim voluntarily reports all the information to the scammer.

Malware - the creation and spread of viruses.

Illegal content - content that promotes extrem-

ism, terrorism, drug addiction, pornography, the cult of cruelty and violence.

Refiling - illegal substitution of telephone traffic [16]

During the pandemic, experts identify four main causes of such crimes: an increase in the number of people working remotely (using IT but not having the appropriate knowledge and experience), an increase in electronic payments, an increase in phishing attacks; potential opportunity for information and cyberattacks to destabilize the situation [21].

The main shortcoming in the field of prevention of negative manifestations of the above cybercrimes is the lack of systematic work on their detection and overcoming, the presence of only declarative provisions in strategies (they can not be different, which is understandable) and the lack of laws and regulations to specify and develop them. low level of public awareness of possible threats (it is worth noting the positive work of some banks in this area), as well as high latency of crimes in this area, which makes it impossible to identify and prosecute all perpetrators.

Another type of cyber conflict is cyberterrorism. Scientific and technological progress, creating new information technologies, in a short time revolutionized the processes of creation, collection, receipt, storage, use, dissemination, protection, protection of information. Today, its results are often used by criminals. Penetration into the information sphere and its use by criminal, including terrorist elements has given rise to phenomena called cybercrime and cyberterrorism. Cyberterrorism - "attacks" on computer systems. The means and methods of cyberattacks have long been mastered by both international extremist organizations and national separatist movements. The first examples of "computer terrorism" appeared in the late 1990s, due to the development of computer networks and the growing role of computers in all spheres of life. As a result, they have attracted the attention of various "cyber-hooligans" and "cyber-terrorists" who carry out attacks through unauthorized access to interfere with the normal operation of relevant institutions [22, p. 100].

Cyberterrorism means a deliberate motivated attack on information processed by a computer, computer system or network that endangers the life and health of people or the occurrence of other serious consequences, if such actions are committed to violate public safety. , intimidation of the population, provocation of military conflict [23].

The Center for Strategic and International Studies defines cyberterrorism as the use of computer network tools to shut down critical national infrastructure (including energy, transportation, government), or to coerce or intimidate government or civilians. Diorditsa I. believes that cyberterrorism should be understood as an illegal act committed with the aim of achieving negative consequences, such as obtaining material benefits or threatening the information security of the state [25]. Cyberterrorism takes place in cyberspace.

Regarding the issue of cyber-conflict prevention, some aspects of this problem have already been disclosed in our previous research. In particular, attention was focused on the need to improve the culture of cybersecurity and learn from the experience of leading countries and harmonize existing legislation with EU regulations [26, p.114].

The choice of negotiations as a way to resolve cyber-conflicts is problematic, but it does not preclude a diplomatic approach. In any case, it is very difficult to maintain strategic stability in cyberspace. Because technological innovation is faster than in the nuclear field, cyber-conflicts are characterized by increased mutual fear of unpredictability. Moreover, as states and organizations begin to better understand the limitations and uncertainties of cyberattacks and the growing importance of Internet interweaving for their economic well-being, the cost-effectiveness calculations of cyber-conflict may change. However, at this stage, the key to prohibition, conflict management and de-escalation in cyberspace is the recognition that we all have much to learn and expand the process of communication between opponents [27].

CONCLUSION

The international community has not yet developed a mutually agreed set of principles, rules and norms that would regulate cyber-conflicts at the international level. It is obvious that most cyber-conflicts have not crossed the boundaries of the generally accepted provisions of "armed conflict", "use of force", "armed attack", etc., they are biased or latent. Here we can talk about the following possible consequences: first, there will be many opportunities for cyber-conflict due to unresolved. Second, the nature of the world community's response to such cyber-conflicts will be uncertain, suggesting a possible freeze or lack of rapid action to resolve cyber-conflicts that are difficult to predict.

As for our state, over the last year certain measures have been taken to resolve cyber conflicts. Thus, the Decree of the President of Ukraine put into effect the decision of the National Security and Defense Council to establish cybertroops in the structure of the Ukrainian Ministry of Defense. It remains to find funds for their formation, as this year's state budget does not provide funds for this. Therefore, the Cabinet of Ministers will have to urgently seek additional money to launch the process of creating Ukrainian cybertroops, which are essential to protect themselves from potential computer threats. However, when forming this structure, it is necessary to clearly state its functions, that they were not duplicated with the functions of other security structures. Here it is worth drawing on the experience of foreign countries, in particular Estonia, which has already created its own cyber troops.

Another aspect of the problem of resolving cyber conflicts is the proper training of specialists who will work in the established security structures, an effective training system, and so on.

The issues of rapid exchange of information on cyber threats and creation of an effective model of public-private partnership are also relevant. In this context, the focus should also be on cyber-security research.

Another important point in the prevention and resolution of cyber-conflicts is the observance of cyber hygiene rules, which should be taught to everyone, from children in kindergarten to presidents, prime ministers, and deputies. Today, the responsibility for the emergence and spread of cyber-conflicts should be borne not only by the state, but also by each of us, because we worry about whether our data has leaked into the network, we forget to behave properly so that data does not leak from our gadget.

REFERENCES

1. Filinovych, V. V. (2020). Problems of human rights violations caused by cybercrimes and ways to overcome them. Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law", 3(56), 143–148. DOI: https://doi.org/10.18372/2307-9061.56.14904
2. Razmetaeva Yu.S. The system of international security in the light of cyber threats: problems and prospects URL: https://dspace.nlu.edu.ua/bitstream/123456789/9804/1/Razmetaeva.pdf
3. Maskun S. H. LL.M Cyber Security: Rule of Use Internet Safely. Journal of Law, Policy and Globalization. 2013. Vol.15. P, c. 22
4. Dubov D.V. Cyberspace as a new dimension of geopolitical rivalry: a monograph. K. : НІСД, 2014. 328 с.
5. Kenneth Geers. Cyber War in Perspective: Russian Agression against Ukraine. – NATO CCD COE Publications, 2015. 175 p.
6. Cyberconflict and geopolitics - a new front of the Cold War. URL: Геополітичний щоденник Віктора Гвоздя http://bintel.com.ua/uk/)
7. 90% of cyber attacks in Ukraine are related to Russia and hacker groups funded by the Russian government - the head of the State Special Service. URL: https://armyinform.com.ua/2021/06/90-kiberatak-v-ukrayini-povyazani-z-rf-i-hakerskymy-grupamy-yaki-finansuye-rosijska-vlada-golova
8. Herber Lin. Cyber conflict and international humanitarian law. – International review of the Red Cross, 2012. pp. 515–531.
9. Peleshchak OR Terminological problems of the cybersecurity sphere of Ukraine: normative-legal aspect. Scientific Bulletin of Lviv State University of Internal Affairs. №4. 2016, C. 299-308 URL: https://www.lvduvs.edu.ua/en/documents_pdf/visnyky/nvsy/04_2016/16pornpa.pdf
10. Cybersecurity strategy of Ukraine. Safe cyberspace - the key to successful development of the country: Decree of the President of Ukraine of August 26, 2021 № 447/2021 URL: https://www.president.gov.ua/documents/4472021-40013
11. Latvian K.V. Forensic characteristics of cyber vandalism. Scientific Bulletin of Public and Private Law. Issue 5, Volume 3, 2018. C. 117-121 URL: http://www.nvppp.in.ua/vip/2018/5/tom_3/25.pdf
12. On the Basic Principles of Cyber Security of Ukraine: Law of Ukraine of 05.10.2017 №2163-VIII, Revision of 01.08.2021, Bulletin of the Verkhovna Rada (BBP), 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#n14
13. Diorditsa IV The concept and content of cyber espionage. Scientific works of the National University "Odessa Law Academy" Volume 26 (2020): DOI: https://doi.org/10.32837/npnuola.v26i0.660 URL: http://npnuola.onua.edu.ua/index.php/1234/article/view/660
14. Cybercrime. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_prytula_cybercrime/
15. Criminal Code of Ukraine: Code of 05.04.2001 №2341-III. Update date: 04.10.2021 https://zakon.rada.gov.ua/laws/show/2341-14#Text
16. Appetite Anastasia. Anatomy of cybercrime: key trends of 2020 / URL: https://ecpl.com.ua/news/anatomia-kiber-zlochynu/
17. On Copyright and Related Rights: Law of Ukraine 3792-XII, current, Date of update: 14.08.2021, URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text
18. On state support of cinematography in Ukraine: Law of Ukraine of March 23, 2017 № 1601-VIII. Update date: 16.07.2020. URL: https://zakon.rada.gov.ua/laws/show/1977-19#Text
19. On e-commerce: EU Directive of 08.06.2000 року № 2000/31/EC URL: https://zakon.rada.gov.ua/laws/show/994_224#Tex
20. On copyright in the digital single market: EU Directive of 17.04.2019 № 2019/790/ЄС URL: https://library.vn.ua/news-and-events/novini/kviten-2021/direktivi-es-pro-avtorske-pravo
21. COVID-19: key cybersecurity trends. URL: https://niss.gov.ua/doslidzhennya/informaciyna-politika/covid-19-klyuchovi-kiberbezpekovi-trendi?fbclid=IwAR3zKcok3HNjQZFuZSZ23heLK9p7L87vizSrTU_Ytp2iPBhndUbZfT8N1RU
22. Terrorism: theoretical and applied aspects: a textbook / col. authors; for the head ed. prof. V.K. Grishchuk. Lviv: ЛьвДУВС, 2011. 328 с.
23. Topchiy V.V. Cyberterrorism in Ukraine: the concept and prevention of criminal law and criminological means. URL: http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf
24. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: James A. Lewis. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
25. Diorditsa IV The concept and content of cyberterrorism. URL: https://goal-int.org/ponyattya-ta-zmist-kiberterorizmu/
26. Sopilko I.M. Information security and cybersecurity: comparative legal aspect. Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law",2021. 2(59). C.110–115. DOI: https:// doi.org/10.18372/2307-9061.59.15603
27. Joseph Nye Is Cyber Warfare Regulated? October 9, 2019 - URL: https://day.kyiv.ua/uk/article/den-planety/chy-piddayetsya-regulyuvannyu-kiberviyna