Safeguarding against cyber threats: Legal measures for ensuring cybersecurity

Oleksandr Skrypniuk | Liudmyla Falalieieva | Oleksandr Chumak | Myroslav Buryk

Abstract The evolution of information technology has defined a new concept for society - cyberspace. Cyberspace is described as a channel for creating and disseminating various data types on the Internet. In addition to providing information, cyberspace contains several problems that require efforts, resources, and the introduction of legal measures. The relevance of the study on this issue is stipulated by the development of information technologies and the high risks that occasionally manifest themselves as cyberattacks. Cyberattacks cannot be limited or deterred, but they can be protected against. For this reason, one of the main priorities for the state nowadays is to protect the information sphere from cyberattacks and cyber threats, as well as to introduce adequate mechanisms to reduce these risks at the legal level. When studying the issue of cybersecurity, it is essential to emphasize how this type of security matters no less than national or internal security. As Ukraine moves closer to the EU, it is crucial to strengthen the facilitation of protection against cyberattacks. It is also essential to find effective methods and tools to not only preserve sensitive information but also to help restore lost resources quickly and efficiently. In addition, it is necessary to bring national legislation in line by adopting regulations that can be really useful in countering external threats. Ukraine is currently an active participant in international efforts to counter cybercrime. The country participates in various projects initiated by the EU and NATO, including strengthening security and defense sector protection and joint exercises of security and defense actors as part of collective defense measures. The proper level of cybersecurity in the country determines society's standard of living and development. For this reason, special attention should be paid not only to the means and methods of protection against cyber threats and attacks but also to the relevant legislative elaborations.

Keywords: cyberattack, cyber threat, cybersecurity, legislation, information space, EU law, EU directives

1. Introduction

Cybersecurity is not a new concept in the Ukrainian legal framework. The development of information technology, the digitalization of information, and the transfer of government functions to smartphones have significantly increased a variety of external hostile influences. They aim not only to obtain confidential information but also to misuse it, causing severe damage. The state policy in the field of cybersecurity seeks to develop appropriate standards and regulations that will strengthen the protection of state institutions from unauthorized information acquisition.

According to Ya.V. Voznenko, a cyber attack is a threat that any organization can face (Voznenko, 2021). According to the results of a global survey conducted by ISACA, only 38% of respondents believe that they are technically prepared for cyber attacks, while 83% believe that these attacks will cause irreparable damage to the organization. In the case of a large volume of personal and confidential information transmitted by electronic means, unauthorized access to it can have serious consequences (ISO/IEC standards, 2016).

The ISO/IES 27032 standard defines "cyber security" as maintaining the confidentiality, integrity, and availability of information in cyberspace. At the same time, cyberspace is an environment that arises as a result of functioning on the basis of uniform principles and general rules of information, telecommunication and information-communication systems (ISO/IES 27032, 2012).
Therefore, ensuring security in cyberspace requires not only state regulation and control, but also conscious and responsible behavior of participants in legal relations, in particular business entities. Currently, in Ukraine, the legislative regulation of cyber protection is just beginning to take shape, having passed a difficult stage of its formation.

2. Literature review

The issue of studying the specifics of cybersecurity and measures and relevant legislative acts to protect against cyber threats and cyberattacks has received insufficient attention. It should be emphasized that a lack of research causes the novelty of this topic. The discussion of cybercrime and cyberattacks began at the end of 2019 when the COVID-19 pandemic spread around the world, and humanity began to use the Internet more actively for personal and business needs.

M.V. Kamchatniy, a Ukrainian scholar specializing in the principles of limiting cyber warfare in the international information space, notes that recent events have significantly increased the problem of countering cyber threats. As this kind of space is new to international law, there is a need to find effective mechanisms to counter cyberwarfare and unauthorized interference in the personal and public information spheres.

V. V. Shemchuk identifies the main directions for Ukraine in strengthening international cooperation in the field of cybersecurity. The author suggests that Ukraine should actively develop and use ICT tools. In turn, V. Pakhomov proposes to systematize the provisions of legal acts regulating the functional and regulatory features of cyberspace as part of countering cyberattacks and cyber threats.

Recent events have shown that the threat of cyberattacks and digital warfare will only increase. Therefore, it is already worth looking for effective mechanisms to address this kind of threat, and this topic should be studied more closely.

This study aims to describe the peculiarities of cybersecurity as well as relevant measures and legislative acts to protect against cyber threats and cyberattacks.

3. Methods

This study is based on a combination of general scientific and special research methods. In particular, the comparative legal method was used to compare the legislation of different countries on the implementation of cybersecurity, as well as to determine the level of protection and the effectiveness of legal mechanisms for countering cyber threats. The systemic-structural method helped to analyze cyber threats and identify effective legal mechanisms that can help overcome these threats. It is worth emphasizing that the application of general scientific and special methods can help to deepen the understanding of the issues and resolve problems related to measures and regulations for protection in the field of cyber threats and attacks.

4. Results

The development of modern innovative technologies is hard to stop. They are developing at a breakneck speed. Their development is influenced by social, political, and economic changes. People have learned to use the Internet for their own needs, business, education, etc. The Internet is a virtual world, just like the real world, but it is virtual. From the comfort of your home, people can chat with friends, hold a meeting, earn money, buy goods, pay for utilities, or do many other things. The electronic network is a tasty morsel for fraudsters who want to harm, hack, or seize valuable information. For the safe use of the Internet, users should follow basic security rules.

Over the years of its independence, Ukrainian society has come a long way in transformation. It has become a modern information society with all the necessary institutions functioning effectively. Information technologies capable of generating a large amount of information are being actively developed and used. However, like anything else, information needs to be protected. Frequent threats to information security threaten not only the destruction of information but also the normal functioning of government agencies, financial organizations, and small and large businesses.

For this reason, it is necessary to provide a secure environment for information. The concept of cybersecurity is understood as the protection of vital interests of a person and a citizen, society and the state in the use of cyberspace, which ensures the sustainable development of the information society and the digital communication environment, timely detection, prevention and neutralization of real and potential threats to national security in cyberspace (Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine"). In the legal environment, there is the concept of national security, which is defined as the state of protection of personal, public, and state interests. Along with national security, it is worth explaining the concept of information security. It is the most common type of security in the state.

According to the Law of Ukraine No. 537-V, information security is defined as a state of protecting the private and public interests of a person, society and the state. Such protection may be caused by incompleteness, untimeliness, and unreliability of the information used, negative consequences of its use, illegal dissemination or disclosure, and violation of the principle of confidentiality and accessibility (Law No. 537-V, 2007).

Article 17 of the Constitution of Ukraine defines information security as one of the most essential functions of the state, imposing the duty to protect it on the people of Ukraine. At the same time, part 2 of Article 34 of the Constitution states that
everyone has the right to information, to collect it freely, to store, use, and spread it orally, in written form, or in any other way (Constitution of Ukraine, 1996).

All over the world, cybercrime causes billions of dollars in losses, destroys the public and private sectors of the economy, and leads to the shutdown of many state institutions, including in Ukraine. Today, in the information legal field, the term “cyber” is mainly related to the use of information technology and computers, i.e., cyberspace and cybersecurity. Cybersecurity is a term based on the need to protect confidential information. Most scholars combine this term with the protection of information in cyberspace without considering the peculiarities of information and psychological confrontation in cyberspace (Melnyk, 2016, p. 192).

Cybersecurity measures are essential as significant volumes of information are stored and transmitted digitally. Such measures include:

- constant use of communication, which involves the use of smart devices and tools that help to collect and organize information and manage it remotely;
- data leaks show the potentially catastrophic consequences of cyberattacks and cyber threats, which ultimately lead to the loss of information and related negative consequences;
- the economic impact is manifested in causing significant financial losses and creating a situation of loss of a considerable amount of resources (Cyber safety Essentials, 2023).

On October 5, 2017, the Law of Ukraine No. 2163-VIII was adopted to provide a legal and institutional framework for protecting the interests of a person and a citizen, society and the state, and the national interests of Ukraine in cyberspace. This normative legal act defines the need to protect the vital interests of a person and a citizen, society, and the state while using cyberspace. It also sets out the peculiarities of ensuring the sustainable development of the information society and the digitized communication environment and timely detection or prevention of potential threats to the national security of Ukraine in cyberspace (Law No. 2163-VIII, 2017).

Shemchuk V. V. states that it is crucial to analyze acts of international organizations on this issue, as well as the changes adopted and the prospects for the very development of cyberspace to determine the direction of Ukraine’s international cooperation with international organizations in the field of cybersecurity (Shemchuk, 2018, p. 128).

Typically, a violation of information space involves cyber influence. It is a purposeful process of using various means, methods, and techniques to attack an enemy’s cyber systems directly. In general, this influence consists of changing the normal modes of their functioning, often to intercept control or bring them under one’s own control, as well as implementing synchronized measures of influence in time. Cyber influence is marked by active actions in cyberspace, i.e., measures of destructive influence on automated control systems, communication systems, navigation and control of weapons, computer networks, or socio-technical systems of the enemy. Modern information technologies are built in such a way that breaking into open information systems with certain skills will be easy (Danyk, 2019).

Bodnar A. O. believes that modern cooperation in the field of ensuring the information security of society between different countries is about finding common solutions that will become an effective means of countering modern information threats, cyberattacks, information terror, and cybercrime (Bodnar, 2020, p. 33). Cybersecurity management in European countries, the United States, Asia, and China has both common and distinctive features. First of all, this can be explained by the peculiarities of the legislative framework and the level of state development. Thus, countries with case law, such as the United Kingdom and the United States, use a risk-based approach to assess cyber threats and the potential danger that these cyberattacks may cause. At the same time, one of the peculiarities of their development and best practices is the absence of a separate legislative document that would regulate cybersecurity in the country. The leading role in these countries is assigned to the actors involved in cybersecurity.

It is worth noting that Israel has a high level of security. This country, with a high level of development, takes great care to protect its information security. Being constantly in a hostile environment, Israel continues to develop high-tech products that are very popular abroad (Best Practices of Cybersecurity Management, 2022, p. 126).

On March 21, 2021, the European Council recognized the need to strengthen cybersecurity at the EU level. The Council also decided to develop policy recommendations to ensure adequate protection for personnel, databases, communication and information networks, and decision-making specifics. The draft legislative initiatives of the European Commission were presented in March 2022, while in June 2023, the Council of the European Union and the European Parliament agreed on the developed legislative proposals. These new regulations are intended to improve the cybersecurity of organizations, institutions, and agencies (New cybersecurity rules came into force in the EU, 2024).

Consequently, cyberspace is an environment where people and the state coexist to a certain extent. Based on best international practices, Ukraine annually reviews, improves, and changes tactics to ensure proper protection of its cyberspace. This indicates that the danger continues, and therefore, protection must be appropriate, sufficient, and timely (Fedchenko, 2017, p. 409).

D. Dubov defines cyberspace as a place created by an organized set of certain information processes based on common principles and rules of information, telecommunication, and information and telecommunication systems, regardless of their ownership (Dubov, 2016, p. 70).

https://www.malque.pub/ojs/index.php/msj
Long before the full-scale invasion, the aggressor state strengthened its cyber influence on government websites, infrastructure facilities, IT networks, and media. These actions were aimed at illegally seizing information related to the principles of government agencies’ work, their facilities, information about employees, etc. Since the beginning of 2014, the armed conflict has been waged not only on the battlefield and in the occupied territories but also in the information and digital space.

The State Special Communications Service is responsible for implementing the state policy on cyber defense. In addition to direct control over the information space, they train specialists who are ready to cope with the current challenges. The enemy’s treachery has no limits, so fruitful cooperation should be a key to the development of the defense sector and information security (Cyber security in Ukraine: ways of development and opportunities, 2023).

Timely implementation of strategic actions is an essential factor in strengthening cyber resilience in order to effectively respond to cyberattacks and cyber threats, as well as to eliminate the preconditions for their occurrence. As part of implementing the Cybersecurity Strategy, the Administration of the State Special Communications Service of Ukraine developed and approved the Methodological Recommendations on how cybersecurity providers should respond to various events in cyberspace (Order No. 570, 2023). This normative legal act defines the peculiarities of influence and regulation of cyberspace, including:

- determination of the necessary list of cyber defense measures taken by security entities to respond to cyber incidents and cyberattacks;
- goals and aims of implementing measures to strengthen countermeasures against cyber threats and cyberattacks;
- principles of prioritizing cyberattacks and cyber threats;
- a typical list of measures to respond to cyberattacks and cyber threats, track them, and take the necessary measures to stop them and eliminate the negative consequences (The SSSCIP has approved the Guidelines for Cybersecurity Actors to Address Various Cyberspace-based Events, 2023).

Awareness of the importance of countering cyberattacks requires the leading European countries to take immediate and decisive actions. For this reason, since the 1990s, EU countries have been actively developing and implementing various developments to strengthen protection against cyberattacks. For a long time, the international community has been discussing the feasibility of regulating cyberspace.

On November 23, 2001, the Convention on Cybercrime (ratified on July 1, 2004) was adopted to regulate cyber threats, fraud, and cybercrime. This international legal document is the first international agreement to regulate violations committed utilizing a computer. The comparison of cybercrime to terrorism indicates the public danger and significant interest of the international community in this issue.

Based on the Convention, a series of directives regulate critical social processes where cyber threats exist. The 2013 Directive on countering cyberattacks and strengthening cybersecurity in the EU is the most important legal act adopted to counter cyberattacks and information systems. The Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union’s financial interests by means of criminal law is also quite effective.

Recently, the intensity of information consumption has only increased. The very process of collecting, storing, processing, and disseminating information in all spheres of society is crucial for the successful solution of political, economic, and other tasks. At the same time, this information can destabilize people, having a detrimental effect on their lives (Nashinets-Naumova, 2017, p. 6).

According to Deputy State Prosecutor D. Verbytskyi, intensive efforts to detect and neutralize cyberattacks are ongoing. At the same time, the official recalled about the destructive, subversive, and disinformation policy that the enemy pursued at the beginning of the full-scale invasion. Together with representatives of the US Department, NATO, and the EU, they discussed joint activities and the international legal framework to strengthen the protection of information systems not only in Ukraine but also in other leading countries. Their experience has shown that Russia is capable of any manipulative steps, which means that protection must be built right here and right now (Verbytskyi, 2024).

5. Discussions

Since the full-scale invasion, more than three thousand cyber incidents and a significant number of cyberattacks have been recorded on the territory of Ukraine (In 2022, 2194 cyber incidents were registered in Ukraine, 2023). Ukraine is currently suffering from multiple cyberattacks from the side of Russian Federation. Personal information of citizens, financial institutions, the public sector, and the defense industry is threatened. Given its achievements, Ukraine continues to confront the enemy in the information field and on the frontline, fighting back with dignity.

Every day, a wide range of organizations, structures, and industries are subjected to cyberattacks. Neither small businesses nor government agencies or educational institutions are immune. During the war, cyberattacks have intensified in the media space. It is quite common for cyberattacks to target the same agencies. Attackers have learned how to use different levels of vulnerability. For example, it is common for attackers to use other persons’ accounts for their attacks. Deputy Head of the State Special Service for Communications O. Potiy notes that Ukraine is the first country in the world to face challenges
when the cyber component is a full-fledged part of the war. The main goal of the state is to prevent the destruction of information systems, including critical infrastructure, to preserve data integrity and citizens' access to various services provided by the state.

Since 2017, after the adoption of the Law of Ukraine, "On the Basic Principles of Cybersecurity in Ukraine," the state has formed a system of state bodies responsible for cybersecurity. Moreover, the country has adopted various regulations and prepared a large number of innovations in the field of information security (Balovsiak, 2024).

Recently, the intensity of information consumption has only increased. The very process of collecting, storing, processing, and sharing information in all spheres of society is crucial for the successful solution of political, economic, and other tasks. At the same time, this information can destabilize people, damaging their lives (Nashinets-Naumova, 2017, p. 6). The state is interested in ensuring information safety, as the stability of society and national security depend on its preservation. Given the events of the last two years, most registries have been disabled to ensure cybersecurity. The intention was to prevent an insidious enemy from gaining access to highly confidential information.

According to the statistics of the General Prosecutor’s Office of Ukraine, as of December 31, 2022, 3415 criminal offenses in the field of information technology were registered. That is 105 more offenses than in 2021. The active spread of cybercrime is facilitated by the hyper-demand for various types of information services in developed countries. In addition, the problems of the large-scale spread of cyberattacks include:

- Globalization of the world economy.
- Development of modern information technologies.
- Uncontrolled use of various electronic information.

The joint struggle to strengthen cybersecurity, as well as the development and implementation of effective methods to prevent cyberattacks, will help solve this problem not only in Ukraine but also in the international arena (Prodan, 2023).

The Verkhovna Rada of Ukraine adopted the Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Improving the Efficiency of Combating Cybercrime under Martial Law" on March 24, 2022, to address the cybercrime level. This law is designed to ensure the reliability and security of digital services, introduce effective criminal law mechanisms to combat crime, and improve the national cybersecurity system (Law No. 2149-IX, 2022).

Specialists of the SSSCIP, together with the EU and the USAID project "Cybersecurity for critical infrastructure in Ukraine" (2022), created and made public the analytical document "War in Ukraine. Pulse of Cyber Defense" (War in Ukraine. Pulse of Cyber Defense, 2022). This document summarizes information about the current level of threats in domestic cyberspace caused by Russia's armed aggression against Ukraine. It highlights the state's activities in the field of cyber defense (How to ensure the protection of Ukraine's cyberspace amid Russia's armed aggression, 2022).

Therefore, the issue of cybersecurity and cyber defense requires not only technical but also functional aspects of cyberspace. First of all, while ensuring cybersecurity, special attention should be paid to such types of protection as legal, organizational, technical, psychological, and informational. Children should be taught to recognize cyber threats as early as they can. The formation of a psychologically and morally stable society is the key to the development of our country (Komykh, 2023).

6. Conclusions

Ukraine is currently engaged in a cyber war. For modern society, cyberspace is a battlefield of hybrid warfare. Cyberattacks on government agencies, organizations, and financial institutions occur daily. The main sectors that the aggressor has attacked are the government and local authorities, the security and defense sectors, and the commercial and financial sectors. One of the most common methods of cyberattacks includes:

- collection of information by the attacker;
- malicious software code;
- intervention;
- known vulnerability.

Once again, it proves the famous fact that cyberattacks are a full-fledged reality of war. Armed conflict itself is a catalyst and a space of opportunity, a condition for strengthening cybercrime through the testing and applying innovative technologies and artificial intelligence.

Further research in the field of cybersecurity is crucial as it affects the effective and full development of all government agencies, institutions, and society in general. Since the beginning of the full-scale invasion, many countries have joined in to strengthen security. Ukraine is cooperating successfully with the United States and European countries, building not only a military but also a significant capacity to combat cyber threats and cyberattacks. Russia continues to wage the armed conflict not only on the frontline but also in the information space, occasionally inflicting attacks.

Currently, Ukraine is actively moving forward, developing and implementing measures and regulations that will help strengthen and prevent cyber criminals from seizing valuable information. As practice has shown, Russian hackers are less strong than the aggressor country's propaganda claims.
Ethical considerations
Not applicable.
Conflict of Interest
The authors declare no conflicts of interest.
Funding
This research did not receive any financial support.

References
In 2022, 2194 cyber incidents were registered in Ukraine (2023). https://susipline.media/397220-u2022-roci-v-ukrainskii-zareestrual-v2194-kiberincident-derszspeczvazku/

https://www.malque.pub/ojs/index.php/msj