Publisher: Sapienza Grupo Editorial
R. Santa Cruz, 2187, Vila Mariana
São Paulo, Brazil
editor@sapienzaeditorial.com

Sapienza
International Journal of Interdisciplinary Studies
ISSN: 2675-9780

Ensuring the functioning of cyberspace in Ukraine: legal and technical aspects

Garantindo o funcionamento do ciberespaço na Ucrânia: aspectos legais e técnicos

Asegurando el funcionamiento del ciberespacio en Ucrania: aspectos legales y técnicos

Iryna Sopilko
https://orcid.org/0000-0001-7670-3157
National Aviation University Kyiv, Ukraine
sopilko8182@edu-knu.com (correspondence)

Valeriia Filinovych
https://orcid.org/0000-0001-8824-615X
Department of Civil Law and Trial
National Aviation University, Ukraine

Olena V. Prudnykova
https://orcid.org/0000-0003-4610-908X
Department of Culturology, Yaroslav Mudryi
National Law University, Ukraine

Anastasiia Krupnova
https://orcid.org/0009-0007-7819-9813
Stepan Demyanchuk International University of
Economics and Humanities, Ukraine

Nataliia Smetanina
https://orcid.org/0009-0002-7834-3436
Department of Criminology and Penitentiary Law
Yaroslav Mudryi National Law University, Ukraine

ARTICLE HISTORY

Received: 26-03-2023
Revised Version: 18-07-2024
Accepted: 02-08-2024
Published: 15-08-2024
Copyright: © 2024 by the authors
License: CC BY-NC-ND 4.0
Manuscript type: Article

ARTICLE INFORMATION

Science-Metrix Classification (Domain):
Economic & Social Sciences
Main topic:
Cybersecurity in Ukrainian Cyberspace
Main practical implications:
The article provides recommendations for enhancing Ukraine's cyber and information security, ensuring its participation in the global information space on equal and independent terms.
Originality/value:
This study integrates legal, technical, and social dimensions of cyberspace, offering an original framework for understanding and securing Ukraine's cyber domain within the broader global context.

ABSTRACT

The authors studied in detail the technical, social, and legal features of the functioning of cybernetic space. The study gives definitions of the cybernetic domain (space) and related terms, such as information space (sphere), cybersecurity, information security, and the like, it indicates goals, objects, and subjects of interaction in cyberspace. Separately considered are its elements such as uncertainty, deterritoriality and the plurality of actors. In the course of this scientific study, the approaches of scholars who researched the cybernetic domain and related categories were analyzed, appropriate conclusions were made on the basis of their work, and the conceptual basis of the work was formed. The authors provide options for solving problems that arise during the use of cyberspace and the information sphere in general, as well as recommendations for ensuring the cybernetic and information security of the state of Ukraine. The methodological basis for this study was the generally recognized criteria of scientific objectivity, as well as other general scientific research methods that provide a comprehensive analysis of cyberspace as an objective new, fourth domain in a range of air, water, and land spaces of Ukraine. The recommendations and suggestions given by the authors of this scientific paper, as well as the conclusions drawn by them, will help coordinate information policy so that Ukraine can become a worthy member of the global information space, and directly cyberspace based on equality and independence.

Keywords: cyberspace, cybersecurity, information security, information space, national security, cyber threat.

RESUMO

Os autores estudaram detalhadamente as características técnicas, sociais e legais do funcionamento do espaço cibernético. O estudo oferece definições do domínio cibernético (espaço) e termos relacionados, como espaço (esfera) de informação, cibersegurança, segurança da informação, entre outros. São indicados os objetivos, objetos e sujeitos de interação no ciberespaço. Elementos como a incerteza, a desterritorialização e a pluralidade de atores são considerados separadamente. No decorrer deste estudo científico, foram analisadas as abordagens de estudiosos que investigaram o domínio cibernético e as categorias relacionadas, conclusões apropriadas foram feitas com base em seu trabalho, e a base conceitual do estudo foi formada. Os autores fornecem opções para resolver problemas que surgem durante o uso do ciberespaço e da esfera de informação em geral, bem como recomendações para garantir a segurança cibernética e informacional do estado da Ucrânia. A base metodológica deste estudo foi fundamentada nos critérios geralmente reconhecidos de objetividade científica, bem como em outros métodos gerais de pesquisa científica que proporcionam uma análise abrangente do ciberespaço como um novo, objetivo e quarto domínio numa gama de espaços aéreo, aquático e terrestre da Ucrânia. As recomendações e sugestões dadas pelos autores deste trabalho científico, bem como as conclusões por eles alcançadas, ajudarão a coordenar a política de informação para que a Ucrânia possa se tornar um membro digno do espaço de informação global e, diretamente, do ciberespaço, baseado na igualdade e independência.

Palavras-chave: ciberespaço, cibersegurança, segurança da informação, espaço de informação, segurança nacional, ameaça cibernética.

RESUMEN

Los autores estudiaron en detalle las características técnicas, sociales y legales del funcionamiento del espacio cibernético. El estudio ofrece definiciones del dominio cibernético (espacio) y términos relacionados, como espacio (esfera) de información, ciberseguridad, seguridad de la información, entre otros. Se indican los objetivos, objetos y sujetos de interacción en el ciberespacio. Se consideran por separado elementos como la incertidumbre, la desterritorialización y la pluralidad de actores. En el transcurso de este estudio científico, se analizaron los enfoques de los académicos que investigaron el dominio cibernético y las categorías relacionadas, se sacaron conclusiones apropiadas sobre la base de su trabajo y se formó la base conceptual del estudio. Los autores proporcionan opciones para resolver problemas que surgen durante el uso del ciberespacio y la esfera de la información en general, así como recomendaciones para garantizar la seguridad cibernética e informativa del estado de Ucrania. La base metodológica de este estudio se fundamentó en los criterios generalmente reconocidos de objetividad científica, así como en otros métodos generales de investigación científica que permiten un análisis exhaustivo del ciberespacio como un nuevo y objetivo cuarto dominio en una gama de espacios aéreos, acuáticos y terrestres de Ucrania. Las recomendaciones y sugerencias ofrecidas por los autores de este documento científico, así como las conclusiones a las que llegaron, ayudarán a coordinar la política de información para que Ucrania pueda convertirse en un miembro digno del espacio de información global y, directamente, del ciberespacio basado en la igualdad e independencia.

Palabras clave: ciberespacio, ciberseguridad, seguridad de la información, espacio de información, seguridad nacional, amenaza cibernética.

INTRODUCTION

The information sphere has become a platform for the development of a post-industrial society and as a catalyst for the creation of an information society in Ukraine. This sphere has a significant impact on the state of economic, political, defense, and other components of the national security of Ukraine. That is why the formation and development of stable and open information space are essential in the creation and development of equally stable cyberspace (*Mitra, 2013*), where information flows freely. Similarly to other countries, Ukraine faces complex cybersecurity challenges. The growing number of cyber threats, including cyberattacks on government and commercial systems, stipulates a need for effective strategies and measures to protect national cyberspace.

Since 2014, Ukraine has been battling against the aggression of the Russian Federation, defending its territorial integrity and sovereignty in every possible way. The enemy is waging war in all dimensions - on land, water, in the air, and cyberspace. However, the first attacks on the information and cybernetic systems of Ukrainian private enterprises and state institutions were committed back in 2013, during the Euromaidan.

In this connection, in the digital age, cybersecurity has become one of the essential components of national security. The increasing number of cyberattacks, data theft and other criminal acts in cyberspace requires a comprehensive approach to protecting information systems and networks.

As the head for the development of electronic services of the Ministry of Digital Transformation Banik notes, this cyber war is generally the first one in the world (Bohdanyok, 2022). Concerning the scale of cyber warfare, the Russian-Ukrainian war is the first one of such a massive extent. Nevertheless, one of the first known examples of cyber warfare is Stuxnet, which was created jointly by the US and Israeli intelligence services. It was a large cyber weapon that attacked industrial control systems of the Iranian nuclear program. At the same time, as Zetter points out, the Russian-Ukrainian cyber war is the first conflict in the cybernetic domain, in which an attack was carried out on the energy system with its subsequent disabling (Zetter, 2016).

In 2017, Ukraine was subjected to large-scale cyberattacks in connection with the rampant Petya virus. This attack made the state authorities regulate the sphere of cyber security. Thus, special legal acts were adopted to ensure the protection of Ukraine's national interests in cyberspace and the implementation of an appropriate state policy on cybersecurity. Even more serious consequences were brought by the actions of the Russian Federation, which launched a hybrid war against Ukraine. However, this case also proves that cyber wars concern not only specific states, but the whole world which should fight against cyberattacks.

As for Ukraine, with the start of a full-scale invasion of Russia on February 24, 2022, the number of cyberattacks has increased significantly. Over the past two years, some Ukrainian state sites have been hacked or attempted to hack, in particular, the web resources of the Ministry of Education and Science, the Ministry of Foreign Affairs, and the Diya service. Attackers used WhisperGate software that can destroy data.

Moreover, on February 15, 2022, a huge DDoS attack was launched by Russia against the websites of the Ministry of Defense, the Ministry of Internal Affairs, and several Ukrainian banks, including Oschadbank (Ukrainska Pravda, 2022). After that, the Ministry of Digital Transformation called on everyone to join the IT army to deter the enemy's attack on the state of Ukraine (Bohdanyok, 2022).

In November 2022, the head of the Cybersecurity Department of the Security Service of Ukraine, Vityuk, reported that the Russian Federation was accompanying its missile strikes against Ukraine's energy facilities with the strongest cyberattacks to create the maximum "blackout" in Ukraine. He also noted that most cyberattacks are not reported to the public although the enemy carries out an average of more than 10 of them per day in the cybernetic domain of Ukraine. This can have a very serious negative impact since such cyberattacks can be more effective than rocket raids because a "simultaneous attack on all regional energy systems can turn off the power throughout the country". Moreover, while about 90% of all cyberattacks come from Russia, 10% of them is realized by the Belarusian special services for the benefit of the Russian Federation. Vityuk noted that about 800 cyberattacks were recorded in 2020, about 1,400 cyberattacks were registered in 2021, while in 2022, their number increased to 3,500 cyberattacks (Ukrainska Pravda, 2022).

All this confirms the need to maintain the high-quality functioning of cyberspace in Ukraine. Thus, it is important to understand the essence of this term, its features, technical structure, and its legal status. In addition, there is an increasing need to reform the Ukrainian legislation to protect cyberspace against Russian cyberattacks.

The purpose of this article is to analyze legal and technical aspects of ensuring the functioning of cyberspace in Ukraine. The research considers the current legislation and regulations governing cyberspace, as well as existing technical means and strategies for protecting information systems. In this regard, the study is aimed to identify shortcomings in the modern cyber defense system and develop recommendations for strengthening cybersecurity in Ukraine. By considering the

Ukrainian legislation on cybersecurity, the key challenges and opportunities in the field of cybersecurity of Ukraine are identified. Moreover, the article analyzes the effectiveness of legislation, the use of technological innovations in cyber defense, the identification of cyber threats and their trends, and specialized personnel training. The study also takes into account the international context and opportunities for cooperation with international partners to ensure the sustainability of Ukraine's cyberspace. Accordingly, recommendations on improving legislation, introducing advanced technologies, strengthening cyber protection of critical facilities and developing cybersecurity personnel are suggested.

So, achieving the research goal - disclosure of all the fundamental components of cyberspace and development on its basis of suggestions for improving the current Ukrainian legal regulation in this area - will be facilitated by the mentioned knowledge gained during this study. Accordingly, the main issue that researchers are trying to solve in this scientific article is improving the legal basement for the functioning of cyberspace in Ukraine, considering its technical aspects.

Consequently, the research purpose leads to the research question of identifying current challenges and problems in cybersecurity in Ukraine and proposing effective measures to enhance cyber defense. Therefore, consideration of the legal and technical aspects of cyberspace is a step towards strengthening Ukraine's cybersecurity and ensuring the stability of the national information space. Given the growing number of cyber threats, this article may be useful for civil servants, cybersecurity experts, academic researchers and anyone interested in cybersecurity in Ukraine. This article offers an integrated approach to the study of the cybersecurity in Ukraine, which makes it scientifically significant and relevant.

Literature Review

The review of domestic and foreign related literature includes publicly available academic articles in Slovenian, Croatian and other languages. Understanding the sense of cyberspace will allow for a deeper analysis of cyberattacks and ensure cybersecurity more efficiently. Although there is certain research of information and cybernetic spheres, there is still a lack of comprehensive studies on cyberwars since they are relatively new in the state of Ukraine.

So, Furashev explores the essence of cyberspace and information space and provides a definition of the concepts of cybersecurity and information security. Thus, he perceives the cybernetic domain as a form of coexistence of material and non-material objects and methods aimed at developing, perceiving, processing, exchanging, and remembering data (Furashev, 2012). Smovzhenko, Skrynnyk, and others describe features of the information-global social reality, functioning in real-time, as one that turns humanity into an integral system of worldwide communication. They also suggest the principles of information policy in Ukraine and define the information space as an umbrella term for the cyberspace (Smovzhenko & Skrynnyk, 2015; Tsypko et al., 2019).

Girich and Chuprina studied the role of information and communication technologies in the daily life of the world community. In addition, they explore the global information space as a bunch of information resources and infrastructures that make up computer webs and other cross-border data transmission channels (Girich & Chuprina, 2007). Furthermore, the influence of the global information space on the state-building is analyzed by Proskurina. She also specifies how state institutions and political organizations are integrated into the global information space. The scholar also focuses on the features of the information strategy of Ukraine in the modern geopolitical space (Proskurina, 2009). Sopilko (*2021*) defines the concept of information security and describes this phenomenon in the framework of information warfare.

At the same time, Weiss and Biermann describe in detail the phenomenon of protecting critical infrastructure from cyberattacks as the main political task of every government and at the same time a public one (*Weiss & Biermann, 2021*). Guo and others study the relationship between cyberspace and real space, assess the situational state of cyberspace, point out the role of network event propagation and traceability analysis, and situational modeling of cyber events to predict risks in cyberspace. They also provide a very clear definition of cybernetic geography (Guo et al., 2019).

Moreover, Medeiros and Goldoni consider cyberspace as a strategic area for international relations in the form of an analytical tool called "The Fundamental Conceptual Trinity of Cyberspace", considering such characteristics of the cybernetic domain as deterritoriality, a plurality of actors, and uncertainty (Medeiros & Goldoni, 2020). Hollis pays special attention to the technical architecture that ensures the functioning of the global Internet and governance in cyberspace and points to the role of international law in cyberspace (Carnegie Endowment for International Peace*, 2021*). Apart from that, Folsom defines cyberspace as an exemplified switched network for the movement of data traffic, which is characterized by degrees of admission, navigation, information action, and development. Consequently, Folsom suggests amendments to legislation in order to respond effectively to new technological challenges (Folsom, 2007).

As noted by Shanker and Usha, cyber technologies have led to an increase in individual digital dependency and reliance on digital technologies, which, in turn, causes data leaks and cyberattacks (Shanker & Usha, 2017). Furthermore, Polanski claims that international customary law should include cyberspace because the Internet is a separate branch of international law in which new norms of customary law arise (Polanski, 2017).

Furthermore, Wu considers human-made attacks to be the external causes of most cyber threats. At the same time, he calls backdoors and vulnerabilities in the target systems as their internal causes ("endogenous security problem"). Accordingly, to eliminate cyber threats, it is necessary to completely exclude endogenous security problems, because external factors can act only through internal ones. However, their complete elimination is impossible because one state will not be able to achieve full independence and control over innovation and industrial chains. This, in turn, stipulates the need for more effective theoretical and technical solutions to eliminate vulnerabilities arising from software and hardware flaws. Moreover, attempts to eliminate these problems contradict both the objectivity of human cognition and modern technological development law. Therefore, it is impossible to guarantee the absence of endogenous security problems in cyberspace (*Wu, 2022*).

Hence, to counter cyber problems, Lei Zhang and others (2022) propose a model of an attacker-defender game in cyberspace, where the state will change depending on the actions of the attacker and the defender, who are colluding with the common goal to maximize rewards. These sources provide a general overview of the current state and prospects of cybersecurity in Ukraine and the world. However, they are not exhaustive, which in turn determines the relevance of this research.

METHODOLOGY

The authors used a qualitative research approach, through which a systematic review of domestic and foreign professional literature on publicly available databases and sources was carried out. Within this approach, such general scientific methods of cognition as analysis and synthesis were applied. They allowed to establish the connection between cyberspace and information space, cybersecurity and information security and other related categories. Moreover, by using these methods, strategic documents were analyzed, such as the national cybersecurity strategy and other political documents that determine strategic priorities in cybersecurity.

One of the leading research methods is the formal legal method. Thus, a rigorous analysis of the current legislation of Ukraine on cybersecurity, including the Constitution, laws, regulations and provisions of relevant industries, was carried out. Method of systematization and generalization facilitated outlining and codification scientific, regulatory and other sources of information on cybersecurity. These methods allowed not only to identify the problems of the current legal regulation of cyberspace, but also to develop a set of recommendations to overcome the gap in this sphere.

The modeling method was the basis for the development of recommendations and proposals for improving legislation on cybersecurity and information security, as well as the functioning of cyberspace in Ukraine. Therefore, it is proposed to use reinforcement learning, which would help identify possible cyberattacks and enhance protection policies.

With the help of a bibliographic review and legal analysis, an attempt was made to define cyberspace, conceptualize it, and determine its distinctive technical, social, and legal components. This will help improve existing local legislation and promote a holistic and strategically oriented understanding of the role of cybernetic domain in the life of the international community.

The analysis of various definitions of cyberspace suggests that its understanding is based on the functional essence of the digital space. Although cyberspace is a more multifaceted phenomenon that harmoniously combines resource, technical, and intellectual elements, whose essence, features, and content can be the subject of further scientific research with an eye to processing and improving legal regulation on this issue.

These methods used made it possible to carry out a comprehensive analysis of the legal and technical aspects of cybersecurity in Ukraine and provide a basis for developing recommendations for improving the protection of its cyberspace.

RESULTS AND DISCUSSION

Cyberspace today is a unique and not fully explored channel for the creation and dissemination of all kinds of information. It has become the main catalyst for world economic growth, an effective way for international dialogue and cooperation, as well as a completely new area of state sovereignty (*Cherniavskyi et al., 2019*). However, it also poses some challenges. Accordingly, the intangible nature of the studied cyberspace complicates the substantiation of its legal foundations with their subsequent normative consolidation in official state sources. In this regard, it can be claimed that the national legislation of Ukraine on cyberspace is represented by the Law 2163-VIII On the Basic Principles for Ensuring Cybersecurity of Ukraine of October 05, 2017. This normative act regulates the basis for ensuring the protection of the country's national interests in cyberspace and the vital interests of a citizen, society, and the state. Its action also extends to the key goals and directions of state policy, the powers, and principles of the activities of state bodies and institutions to ensure cybersecurity. Article 1 (paragraph 11) of Law 2163-VIII defines cyberspace as a virtual domain created to manage connected, compatible communication systems and electronic communications using global information transmission networks (Ukrainian government, 2022). Thus, cyberspace is an ever-evolving environment that changes as technology advances and adapts to new emerging user needs. Due to the ongoing technological progress and increasing user experience, it is characterized by constant variability.

Moreover, the information component of cyberspace is also important. So, it is distinguished by the absence of geographic reference and the boundaries of physical space, displaying its transboundary character. Apart from that, the cybernetic domain does not exist on its own, it is inextricably linked with the information sphere (environment). Within this research, it is also important to understand its essence. Thus, Section I of Law No. 537-V On the Basic Principles for the Development of the Information Society in Ukraine for 2007-2015 dated January 9, 2007 defines one of the main priorities of the Ukrainian state as the formation of an information society that will be open to everyone and focused on the interests and development of individuals. In such a society, each person will not only receive knowledge, but also produce it, transfer it to other people and social groups, freely access such information. As a result, every Ukrainian will be able to fully realize one's potential, which will improve the quality of life and promote development of society (*On the Basic Principles for the Development…, 2007*).

The organizational and legal foundations for developing the information society in Ukraine are enshrined in paragraph 3 of Section IV of Law No. 537-V, which include resource, institutional, and integration. In this regard, in order to integrate Ukraine into the global information space, it is important that Ukraine participate in international cooperation on reducing the digital and information divide in society. In addition, the Law prescribes the integration of Ukrainian science and culture into the global scientific, technological, and cultural information space, as well as encouraging partnerships between all sectors of the economy to develop the information society, as required by the UN Millennium Declaration (*On the Basic principles for the development…, 2007*). Moreover, the entry of the Ukrainian state into the world information space and information-oriented interstate cooperation is indicated as one of the main directions and priorities of state policy in paragraph 8 of part 1 of article 3 of Law No. 2657-XII "On Information" dated October 02, 1992 (*On information, 2022*).

Furthermore, the global information space is considered an important element of the social space, even as a kind of special "social information space". As Proskurina comments, while implementing the information strategy, an important direction for Ukraine should be the active participation in the work of international organizations aimed at the regulation of the global information space. Therefore, Ukraine should join international treaties on the procedure for the activities of official and non-official bodies in information networks (*Proskurina, 2009*). However, some scientists proceed from the fact that the global information space should be regarded as a set of information resources and infrastructures with interstate and state computer networks in their composition. This set also includes public networks, telecommunications systems, and other cross-border data communication channels. These resources are websites, various texts, databases, and other content that form a single information space through the information and communication infrastructure (*Girich & Chuprina, 2007*).

At the same time, there is another point of view that combines several equivalent approaches to the definition of the information environment (space, field), regarding it as follows:

- A sphere of subjective activity where data are produced, consumed, and altered;
- A similar sphere of subject activity within the framework of public life which also includes the preservation of information, its dissemination, and processing;
- The plurality of the knowledge and information, the information infrastructure, and the subjects carrying out information activities;
- A set of systems of information resources, the interaction of information, and information infrastructure (*Smovzhenko & Skrynnyk, 2015*).

In the field of standardization, CNSSI 4009-2015 of the Committee on National Security Systems was adopted (*Committee on National Security Systems…, 2022*), which defines the information environment as a set of people, organizations, and systems that manage, process, disseminate information, or affect it (*Girich & Chuprina, 2007*). At the same time, it is important to pay attention to the fact that the information space is not static; it is also clearly structured with the help of information fields and flows. However, information has no physical boundaries but has an objective virtual component.

Consequently, the terms "cyberspace" and "information space" are not identical although they are very similar. Thus, cyberspace is an inseparable element of the information space, covering only people that perceive, process, recall data, and exchange acquired knowledge. Meanwhile, the information space (information environment) applies to all sources of information in general, when the subjects of interaction are not required to appropriately perceive data, exchange and process them.

At the same time, according to Furashev, these concepts are characterized by such signs as the reality of a generally acting impact, the simultaneous combination of material and non-material, discrete and constant, abstract and real (*Furashev, 2012*). Nevertheless, cyberspace and information space are different concepts. Thus, in authors' opinion, the first should be considered an element of the second, an important segment in which global economic and political flows and social relationships are concentrated. In this regard, cyberspace have the following characteristics: deterritoriality, multiple actors, and uncertainty. Medeiros and Goldoni claim that each of these characteristics do not pose a problem, but when they act together, they can cause problems. Unlike traditional spaces, cyberspace is not limited by territorial boundaries. It is essentially intangible, yet dependent on mobile devices operating in traditional spaces. Hence, it is possible to conclude the simultaneous "presence" of cyberspace in physical spaces through the information flows of the electromagnetic spectrum.

The deterritorializing nature of cyberspace is manifested in its partial non-materiality, but such a space is both an object and a means of power relations. When the relevant subjects use it for their selfish purposes, the territorialization of cyberspace occurs. In this regard, some challenges arise regarding the zonal logic of the territory as a geographical contour in which the state exerts its dominant influence by controlling border flows. The multiplicity of actors in cyberspace is manifested in the fact that it has become a platform for power relations, and the number of actors able to access and interact with this new seat of power is constantly growing. Low costs of use contribute to this factor (*Medeiros & Goldoni, 2020*).

This multiplicity resulted in an opportunity for intelligence agencies to track the conversations of state authorities, businessmen, and researchers in all corners of the planet; terrorists can recruit novices from other lands; hackers can cause significant physical damage to the critical infrastructure of the state. The low cost of use allows cybercriminals to commit sabotage easily in the cybernetic domain (for example, against a specific airport, as was the case with Ukraine in 2017 due to the Petya virus), train people, acquire and operate special equipment to destabilize the work of the organization. The situation is aggravated by the fact that the more complex the state infrastructure, the higher the level of its vulnerability to cyber threats.

Uncertainty as a special quality of cyberspace is manifested in the complexity of the process of identifying and recognizing the ownership of actions by specific actors, thus undermining accountability processes. As a result, there is a lack of indicators of success and anonymity in cyberspace (*Vapniarchuk et al., 2019*). Concerning the issue of accountability, there is contextual responsibility, which means that the responsible person is the subject who benefits from the action. As a result, obstacles to the process of attribution and subsequent accountability can lead to an escalation of the war or the prosecution of the innocent (*Medeiros & Goldoni, 2020*).

Furthermore, the main sources of Ukrainian legislation regulating issues of cybersecurity were analyzed. The main Ukrainian legal document that regulates issues related to cyberspace is Law No. 2163-VIII. It defines cyberspace and cybersecurity. Thus, according to paragraph 5 of Article 1 of this Law, cybersecurity represents the protection of the vital interests of the state of Ukraine, Ukrainian society, and directly each inhabitant of Ukrainian territory when operating in cyberspace. This is regarded as a condition for the sustainable development of the Ukrainian information society when the digital communication environment is created. In addition, it provides the identification, precluding, and elimination of possible or real threats to the national security of Ukraine in cyberspace (Ukrainian Government, 2022). It should be noted that state security in the generalized sense usually implies a condition of protection of the state from internal and external threats. It organically combined military, social, economic, and information security.

Information security can be defined as a special state of protection of the information environment of the Ukrainian society, in which its members and the state can freely develop information, being confident in the protection of their information rights from internal and external cyber threats (*Sopilko, 2021*). Paragraph 13 of section 2 of Law No. 537-V gives an official definition of information security as a special state of protection of the interests of Ukraine, every Ukrainian, upon reaching which there will be no harm due to the untimeliness, incompleteness, and inaccuracy of the information provided (*On the Basic principles for the development…, 2007*). As a result, it can be affirmed that cybersecurity is an important element of information security, which in turn is a central segment of national security.

In addition to the Law on Cybersecurity No. 2163-VIII, ensuring the functioning of the cybernetic domain in the Ukrainian state is regulated by other legal acts, namely:

- The Constitution of Ukraine of 1996;
- Laws: "On Information" (dated 02.10.1992 No. 2657-XII), "On the Fundamentals of Domestic and Foreign Policy" (dated 01.07.2010 No. 2017 No. 2163-VIII), "On the National Security of Ukraine" (dated June 21, 2018 No. 2469-VIII), "On Electronic Communications" (dated December 16, 2020 No. 1089-IX) and others;
- International treaties, following the requirements of Article 9 of the Constitution of Ukraine;
- Decrees of the President of Ukraine;

● Acts of the Cabinet of Ministers of Ukraine;

● Other regulatory legal acts.

Consequently, the legal support for the functioning of cyberspace in Ukraine is represented by program and regulatory acts containing tasks, objectives, and means to achieve a suitable level of cyberspace protection. However, in addition to the existing legal framework, the following principles should also be considered, without which, in authors' opinion, it will be challenging to guarantee cybersecurity:

● Respect for human rights and freedoms. The prevention of human rights violations is an essential element of the policy of each state (*Myronets et al., 2019*). According to this principle, all activities of the authorities in cyberspace should be aimed at providing the observance of such rights and interests, and any limitations imposed should not violate them.

● Responsibility. Each participant in a cybernetic domain must be responsible for preserving stability in it.

● Rationality and cognition. Participant of relations in the cyberspace must assume that their actions can threaten the stability of cyberspace;

● Appropriate intervention. In case of non-observance of the previous principle, appropriate measures are needed on the part of the state authorities ensuring the functioning of the cyberspace in Ukraine.

It is also noteworthy that the development of guides and standards is necessary for preventing destabilizing actions, as well as at stimulating the implementation of steps to enhance the stability of cyberspace.

Ensuring the functioning of cyberspace in Ukraine in the context of information hygiene is an extremely important task in the modern digital world. Information hygiene covers a wide range of means to preserve and protect sensitive information, personal data and other valuable assets in an online environment. Ukraine faces growing threats in cyberspace that affect national security, economy and social stability. In the context of information hygiene, ensuring the functioning of cyberspace in Ukraine means the development and implementation of strategies that contribute to the security of information in all spheres of society. This can be achieved through cooperation with international partners to exchange information, experience and technical means in the field of cybersecurity. As a result, it is possible to gain stability and security in the online environment for all citizens and organizations of Ukraine.

Such phenomena as phishing, vishing, and scrolling and other fraudulent methods of social engineering are commonplace in cyberspace due to ignorance of the population and the lack of information literacy. Accordingly, raising public awareness about threats on the Internet and the importance of applying appropriate protection measures among users, enterprises and government bodies is an important aspect in the context of cyber defense. Furthermore, trainings, seminars and cybersecurity education campaigns are effective improvements of information systems security systems, including critical infrastructure. In this regard, it is important to specify the risks and opportunities of cyberspace (Table 1).

Table 1. Main aspects of cyberspace in Ukraine: risks and opportunitie

Aspect	Essence	Current state	Risks and opportunities
Cybersecurity	Global information technology environment for human interaction over the Internet and other networks.	It includes Internet infrastructure, computer systems, embedded processors, telecommunications networks.	- **Risks**: cybercrime, attacks on critical infrastructure, legal uncertainty. - **Opportunities**: Economic growth, global communication, international cooperation.
Information space	A set of information resources and infrastructures, including computer networks, telecommunication systems, databases.	Formation of the information society, integration into the world information space.	- **Risks**: Information war, fake information, digital divide. - **Opportunities**: Development of science and culture, international cooperation, reduction of the digital divide.
National security	Protecting the vital interests of the state, society and citizens in cyberspace.	It includes protection of national interests, prevention and elimination of cyberspace threats.	- **Risks**: Vulnerability to cyberattacks, insufficient regulation. - **Opportunities**: Sustainable development, increasing confidence in the digital environment, strengthening national security.
Economy	Industry funding, state support, investments.	The cybersecurity industry is underfunded by the state and foreign investors.	**- Risks:** scarce resources, insufficient funding. **- Opportunities:** attracting investments, state support.
Politics	The sphere of subjective activity carried out by political leaders and government in the context of cyberspace and the impact of the international situation on cybersecurity.	It includes resources and infrastructures of interstate and state networks; partial support for less developed countries (requires activation); regional instability.	**- Risks:** growth of cyber threats, international conflicts, war. **- Opportunities:** knowledge exchange, cultural integration, support for international security.
Legislation	Norms and acts regulating cybersecurity in Ukraine (Law of Ukraine of No. 2163-VIII "On the main principles of ensuring the cybersecurity of Ukraine", Ukrainian government 2022).	It regulates the protection of national interests in cyberspace, establishes the foundations of cybersecurity. It is underdeveloped, needs updating and harmonization.	- **Risks**: Lack of regulation, lagging behind technological progress, legal gaps, insufficient legal responsibility. - **Opportunities**: Creation of a safe cyber environment, international cooperation in cybersecurity, improvement of legislation and its harmonization with the European standards

Source: Elaborated by the authors with the legal sources of the analysis

Therefore, based on the analysis, the following recommendations can be made to increase the level of cyber defense in Ukraine:

- Strengthening of the national cyber and information security system with the involvement of not only government agencies but also representatives of the commercial and academic spheres;
- Providing an official interpretation and definition of the legal status and position of information resources, taking into account their ownership, the level of protection and access to information;
- Ensuring a balance between the principle of openness of information and the restriction of access to it. Ukrainian society is an information one, and, therefore, the protection of data with limited access is impossible without the development and implementation of a flexible legal framework and a balanced state policy in the information sphere;
- Further implementation of digitalization and the development of a competitive Ukrainian information product;
- Provision of information safety in connection with the dominance of fake data and misinformation. Consequently, it is important to protect society from negative information impact by training the Ukrainians in cyber and information hygiene;
- Counteracting cybercriminals and cyberterrorists in many areas of social interaction, information and telecommunication;
- Formation and promotion of a positive image of the state of Ukraine on the Internet as one that in every possible way supports and helps to develop the information society.

Discussion

The term "cyberspace" refers to some sort of global information technology environment where people communicate, do business, work, exchange information, and interact. This concept, for the most part, has become generally accepted in connection with the use of the World Wide Web. While some researchers determine cyberspace as a part of the national critical infrastructure (*Weiss & Biermann, 2021*), others define it as a phenomenon determined not so much by technical implementation, but by social interaction (*Morningstar & Farmer, 2003*).

In this regard, it is worth noting that at the arch of the present and past centuries, in social and technical sciences, the term "global information space" arose as directly related to cyberspace. This is the result of the widespread and intensive involvement and the use of the latest achievements of the information technology revolution in the world in everyday life. However, a more focused term "global cyberspace" is used.

There are several approaches to defining and understanding cyberspace. For the first time the term "cyberspace" appeared in the book "Neuromancer" by Gibson in 1984. Gibson understood cyberspace as a kind of concerted illusion that a huge number of users on earth experience every day. He strongly criticizes this concept, considering it to be "meaningless". Nevertheless, the term is now widely used to describe objects and functions related to the worldwide global network (*Gibson, 2004*).

From a technical point of view, Hollis understands this concept as the technical architecture that assures the functioning of the Internet as a worldwide global network (Carnegie Endowment for International Peace*, 2021*). The identification of cyberspace with the global Internet network is also observed in Duhem's legal dictionary, where it is called decentralized, but at the same time interconnected by a set of data and an autonomous telecommunications network (Duhaime Legal Dictionary*,* 2022). In addition, the legal dictionary Farlex, when trying to find out the essence of the concept of cyberspace, redirects the user to a webpage dedicated to the term "Internet", which is comprehended as the worldwide telecommunications network employed by state, commercial and private entities (TheFreeDictionary*, 2022*).

Moreover, as Techopedia points out, any system that has a substantial user base or even a well-designed interface can be understood as cyberspace. At the same time, its main feature is an interactive and virtual environment for a wide spectrum of parties (Techopedia*,* 2022). Therefore, Folsom understands cyberspace as a switched network for moving information traffic, which is characterized by different levels of access, information activity, navigation, and trust in it. He does not identify this concept with the Internet, which, in his interpretation, is a special tool that creates and opens the gateway to cyberspace. At the same time, the set of actions that make up cyberspace on the other side of the gateway and the gateway itself constitute an objective cyberspace with matters that can arise from its goals (*Folsom, 2007*).

In addition, Medeiros and Goldoni understand the concept of cyberspace as a unique area of artificial interaction between people, existing in the combination of technological, technical, and personal layers, without which traditional areas are no longer represented. The uniqueness of cyberspace as a domain lies in the fact that, unlike the "physical" ones, it was created by people (*Medeiros & Goldoni, 2020*).

From the scientific point of view, it is also important to consider the definition of cyberspace by Furashev. Accordingly, cyberspace is a form of coexistence of a special bunch of material and non-material objects, phenomena, methods, and strategies aimed at interaction with information. In other words, this is the creation and processing of information and knowledge, as well as their mutual exchange (*Furashev, 2012*).

Hence, it can be concluded that there is no single unified and standardized definition of the term "cyberspace" although the analyzed definitions involve a system of connected computers, digital networks, and other communication and information technologies. Thus, the authors of this article believe that cyberspace is a kind of interactive domain in which data (information, facts, knowledge) is stored, used, processed, operated as an object of exchange and transfer.

The term "cyberspace" in a purely practical plane is mentioned in scientific literature and officially fixed in the domestic legislations. For instance, this term is mentioned in paragraph 8 of the Okinawa Charter of the Global Information Society, which states that the international community should direct its forces and resources to coordinated activity to create not only a secure but also crime-free cyberspace. It is essential for the development of the World Information Society (*Virchow & Braun, 2000*). Cyberspace is also mentioned in the 2015 United States–China Cybersecurity Agreement, in the draft Cyberspace Electronic Security Act of 1999, S.3480 – Protecting Cyberspace as a National Asset Act of 2010. In these regulatory documents, this concept was represented as an interconnected network information infrastructure, the components of which are telecommunication networks, various systems, embedded processors, and controllers used in critical industries (*Lieberman, 2010*).

It is also worth considering the standards for software solutions of the National Institute of Standards and Technology (NIST) and the American National Standards Institute (ANSI) (NIST, 2015). For example, NIST SP 800-30 Rev. 1, NIST SP 800-39, and NIST SP 800-53 Rev. 4 define cyberspace as a global area in the information environment with an interconnected network of information system infrastructures, that is, computer systems, embedded processors and controllers in critical industries, as well as telecommunications networks and the Internet (NIST, 2011; NIST, 2011b;. Organization, Mission, and Information System View, 2011; NIST, 2021). Nevertheless, NIST SP 800-160 considers this term as an interconnected network of information technology infrastructures, which includes not only the already mentioned computer systems, embedded processors, and controllers, but also telecommunications networks along with the World Wide Web (NIST, 2021).

Consequently, it is possible to state that current international law does not contain special norms and rules for regulating relations in cyberspace. In this regard, Hollis points to insufficient regulation of cyberspace within the current international law, although some international organizations such as the Group of Twenty, the First Committee of the UN General Assembly on Disarmament and International Security, and the EU, have developed their legal acts with the applicability of international law in interaction with information and communication technologies. That is, the question concerns not the possibility of applying international law, but how this will be done (Carnegie Endowment for International Peace, 2021).

CONCLUSIONS

In this article, the legal and technical aspects of ensuring the functioning of cyberspace in Ukraine were considered. Analyzing the current legislation, strategies and technical means of cyber defense, a number of problems and challenges in this area were identified. As a result, the need for further improvement of legislation, the creation of effective coordination and control mechanisms, enhancing cyber protection of critical facilities, and raising public awareness were defined as key aspects for ensuring the stability of cyberspace in Ukraine. Moreover, it was established that by improving cyberspace protection, Ukraine will be able to become a worthy member of the global information space.

The suggested recommendations can serve as a basis for further measures and strategies in the field of cybersecurity. Through the joint efforts of the government, the private sector and the public, Ukraine will be able to ensure effective cyber defense and protect its national security in the digital era. Therefore, it was substantiated that the main task of the state authorities consists in continuous updating of strategies and technical means, and advanced training of cybersecurity experts. In this way Ukraine will be able to effectively respond to cybersecurity challenges and protect its interests in the digital world.

Main limitations of the study and future research

Concerning the research limitations, the globalization challenges of cyberwars in terms of cybersecurity was not considered in this article because they are multidimensional and embraces many aspects that should constitute a separate study. Moreover, educational aspect of cybersecurity should be analyzed in more detail since it is necessary to teach children cyber hygiene.

Accordingly, the directions of future research on ensuring cyberspace functioning in Ukraine lies in the study of cyberspace infrastructure in Ukraine and identification of vulnerabilities that can be used by cybercriminals. Apart from that, it is possible to analyze opportunities for deepening cooperation with international partners in order to exchange information and experience in cybersecurity. Finally, further research may also include interviews with experts, analysis of statistical data and examples of best practices for cybersecurity in other countries.

REFERENCES

Bohdanyok O. (2022). This is the world's first cyber war. The Ministry of Digital told about the Ukrainian IT army. In Suspilne News. Retrieved from: https://suspilne.media/222186-ce-persa-u-sviti-kibervijna-u-mincifri-rozpovili-pro-ukrainsku-it-armiu/

Carnegie Endowment for International Peace. (2021). A brief primer on international law and cyberspace (2021). Retrieved from: https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Cherniavskyi, S. S., Golovkin, B. N., Chornous, Y. M., Bodnar, V. Y., Zhuk, I. V. (2019). International cooperation in the field of fighting crime: directions, levels and forms of realization. *Journal of Legal, Ethical and Regulatory*, *22*(3). Retrieved from: https://www.abacademies.org/articles/International-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-1544-0044-22-3-348.pdf

Committee on National Security Systems (CNSS) Glossary (2022). CNSSI 4009. Retrieved from: https://www.serdp-estcp.org/content/download/47576/453617/file/CNSSI%204009%20Glossary%202015.pdf

Duhaime Legal Dictionary. (2022). Cyberspace Definition. Retrieved from: https://www.duhaime.org/legal-dictionary/term/cyberspace

Folsom, T. C. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). *Tulane Journal of Technology & Intellectual Property*, *9*, 75. Retrieved from: https://ssrn.com/abstract=1350999.

Furashev, V. M. (2012). Cyberspace and information space, cybersecurity and information security: essence, definition, differences. *Information and Law*, 2(5), 162–175.

Gibson, W. (2004). Neuromancer: 20th anniversary edition. New York: Ace Books.

Girich, V. L. & Chuprina, V. N. (2007). Global information space and the problem of access to world information resources. Retrieved from: http://marc21.rsl.ru/upload/mba2007/mba2007_05.pdf

Guo, Q., Gao, C., Jiang, D., Wang, Z., Fang, C. & Hao, M. (2019). Theoretical basis and technical methods of cyberspace geography. *Journal of Geographical Sciences*, *29*(12), 1949–1964. Retrieved from: https://doi.org/10.1007/s11442-019-1698-7

Lieberman, J. (2010). S.3480 - Protecting Cyberspace as a National Asset Act of 2010. 111th Congress. Homeland Security and Governmental Affairs. Retrieved from: https://www.congress.gov/bill/111th-congress/senate-bill/3480/text

Medeiros, B. P. & Goldoni, L. R. F. (2020). The fundamental conceptual trinity of cyberspace. *Contexto internacional*, *42*(1), 31–54. Retrieved from: https://doi.org/10.1590/s0102-8529.2019420100002

Mitra, A. (2013). Cybernetic Space. *Journal of Interactive Advertising, 3*(2), 1-9.

Morningstar, C. & Farmer, F. R. (2003). The Lessons of Lucasfilm's Habitat. *The New Media Reader (pp. 664-667).* Cambridge, Massachusetts, London: The MIT Press. Retrieved from: https://monoskop.org/images/4/4c/Wardrip-Fruin_Noah_Montfort_Nick_eds_The_New_Media_Reader.pdf

Myronets, O.M., Burdin, M., Tsukan, O. & Nesteriak, Y. (2019). Prevention of human rights violation. *Asia Life Sciences*, 21(2), 577–591.

National Institute of Standards and Technology (NIST). (2011). Special Publication 800-30. Revision 1. Gaithersburg: National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology (NIST). (2015). Supplemental Information for the Interagency Report on Strategic U. S. Government Engagement in International Standardization to Achieve U. S. . NISTIR 8074. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

National Institute of Standards and Technology (NIST). (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (2021). NIST Special Publication 800-160. Revision 1. Retrieved from: https://doi.org/10.6028/NIST.SP.800-160v2r1

National Institute of Standards and Technology (NIST). (2021). Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision. 5. Retrieved from: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

National Institute of Standards and Technology (NIST)b. Managing Information Security Risk. Organization, Mission, and Information System View (2011). NIST Special Publication 800-39. Gaithersburg: National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

Polanski, P. (2017). Cyberspace: A new branch of international customary law? *Computer Law & Security Review, 33*(3), 371-381.

Proskurina, O. (2009). Information strategy of Ukraine in the modern geopolitical space. *Information Society, 3*, 1–8. Retrieved from: https://ipiend.gov.ua/wp-content/uploads/2018/07/proskurina_informatsina.pdf

Shanker, A. & Usha, G. (2017). Cyber threat landscape in cyber space. In: *International conference of Electronics, Communication and Aerospace Technology (ICECA)* (375-380). Coimbatore: IEEE.

Smovzhenko, T. S. & Skrynnyk, Z. E. (2015). Ukrainian people in the European world: the dimension of identity. Kyiv: UBD NBU. 609 p.

Sopilko, I. M. (2021). Information security as an object of regulation in the law of Ukraine. *Journal of International Legal Communication, 1*(1), 11–22. Retrieved from: https://doi.org/10.32612/uw.27201643.2021.1.

Techopedia. (2022). What Does Cyberspace Mean?. Techopedia. Retrieved from: https://www.techopedia.com/definition/2493/cyberspace

TheFreeDictionary. (2022). Definition of cyberspace. Retrieved from: https://legal-dictionary.thefreedictionary.com/cyberspace

Tsypko, V., Alieksieieva, Kateryna I., Venger, I. A., Tavolzhanskyi, O. V., Galunets, N. I. & Klyuchnik, A. V. (2019). Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction. *Journal of Advanced Research in Law and Economics*, *10*(6), 1664-1672.

Ukrainian Government (2022). Law of Ukraine No. 2657-XII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#text

Ukrainian Government. (2007). On the Basic principles for the development of the information society in Ukraine for 2007-2015 (2007). Law of Ukraine No. 537-V. Retrieved from: https://zakon.rada.gov.ua/laws/show/537-16#text

Ukrainian Government. (2022). On the main principles of ensuring the cybersecurity of Ukraine. Law of Ukraine of No. 2163-VIII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#text

Ukrainska Pravda. (2022). Cyber-attacks on Ukrainian web resources are possible on February 22 – CERT-UA. In Ukrainska Pravda. Retrieved from: https://www.epravda.com.ua/rus/news/2022/02/21/682554/

Ukrainska Pravda. (2022b)Russia daily carries out more than 10 cyber-attacks on strategic objects of Ukraine – SSU (2022). In Ukrainska Pravda. Retrieved from: https://www.pravda.com.ua/rus/news/2022/11/9/7375609/

Vapniarchuk, V. V., Puchkovska, I. I., Tavolzhanskyi, O. V., Tashian, R. I. (2019). Protection of ownership right in the court: the essence and particularities. *Asia Life Science*, *21*(2), 1-19.

Virchow, D. & Braun, J. (2000). Okinawa Charter for the Global Information Society. Geology. Retrieved from: https://www.semanticscholar.org/paper/Okinawa-Charter-on-Global-Information-Society-Virchow-Braun/3eae8bc9b7564b4dd0840d744fad1280038d9131

Weiss, M. & Biermann, F. (2021). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, 1–18. Retrieved from: https://doi.org/10.1080/17487870.2021.1905530

Wu, J. (2022). Cyberspace Endogenous Safety and Security. *Engineering, 12,* 179-185.

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid. In WIRED. Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zhang, L., Pan, Y., Liu, Y., Zheng, Q., & Pan, Z. (2022). Multiple Domain Cyberspace Attack and Defense Game Based on Reward Randomization Reinforcement Learning. *Array, 16,* 100262

Contribution of each author to the manuscript:

	% of contribution of each author				
Task	**A1**	**A2**	**A3**	**A4**	**A5**
A. theoretical and conceptual foundations and problematization:	20%	20%	20%	20%	20%
B. data research and statistical analysis:	20%	20%	20%	20%	20%
C. elaboration of figures and tables:	20%	20%	20%	20%	20%
D. drafting, reviewing and writing of the text:	20%	20%	20%	20%	20%
E. selection of bibliographical references	20%	20%	20%	20%	20%
F. Other (please indicate)	-	-	-	-	

Indication of conflict of interest:

There is no conflict of interest

Source of funding

There is no source of funding

Acknowledgments

There is no acknowledgment