

STRENGTHENING CYBERSECURITY IN UKRAINE: LEGAL FRAMEWORKS AND TECHNICAL STRATEGIES FOR ENSURING CYBERSPACE INTEGRITY

Iryna Sopilko

National Aviation University

03058, 1 Lyubomir Huzar Ave., Kyiv, Ukraine

e-mail: sopilko8182@edu-knu.com

<https://orcid.org/0000-0001-7670-3157>

Abstract

Since 2014, Ukraine has been grappling with increasing cyberattacks linked to ongoing conflicts, notably with the Russian Federation. The study highlights the evolution of Ukraine's cyber defense strategies, including responses to significant incidents such as the 2017 Petya virus attack and the escalation of cyber hostilities following Russia's full-scale invasion in February 2022. The research provides an in-depth analysis of legal measures and technical infrastructure aimed at safeguarding Ukraine's cyberspace. It examines key legal frameworks adopted to enhance cybersecurity, the role of governmental and non-governmental entities, and the technical challenges faced in protecting critical infrastructure from cyber threats. The paper also reviews significant contributions from both Ukrainian and international scholars, offering a comprehensive understanding of cyberspace's multifaceted nature and its implications for national and global security. The paper concludes with strategic recommendations for advancing Ukraine's cybersecurity posture, including the continuous improvement of national security systems, balancing information openness with access restrictions, fostering digital innovation, and enhancing public cyber hygiene. The findings underscore the importance of a cohesive approach to cybersecurity that integrates legal, technical, and societal dimensions to effectively counter cyber threats and uphold national security. By addressing these critical areas, Ukraine aims to establish itself as a resilient participant in the global information and cyberspace community.

Keywords: Cyberspace; cybersecurity; legal frameworks; technical infrastructure; national security.

1. Introduction

Today, the information sphere became a platform for the development of a post-industrial society, it is a catalyst for the formation of an information society in Ukraine. And this sphere has a significant impact on the state of economic, political, defense, and other components of the national security of the Ukrainian state. That is why the formation and development of stable and open information space in the country are what will allow creating and developing an equally stable cybernetic space, where fast and mobile information flows efficiently and freely exist and interact.

As most of the world knows, 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 even in a relatively new one - cybernetics. But the first attacks on the information and cybernetic systems of Ukrainian subjects (private enterprises and state institutions) were committed back in 2013, during the Euromaidan.

The Russian-Ukrainian cyber war, as K. Zetter points out, is the first conflict in the cybernetic domain, in which an attack was carried out on the energy system with its subsequent disabling (Inside the Cunning, Unprecedented Hack..., 2016). At the same time, as the head for the development of electronic services of the Ministry of Digital

Transformation M. Banik notes, this cyber war is generally the first in the world (This is the world's first cyber war..., 2022).

In 2017, Ukraine, in the face of its critical infrastructure facilities, was subjected to large-scale cyber-attacks in connection with the rampant Petya virus. Then the state authorities seriously thought about regulating the sphere of cyber security and threw a lot of effort into resolving this matter. Special legal acts were adopted to ensure the protection of Ukraine's national interests in cyberspace and the implementation of an appropriate state policy in the field of cybersecurity. Even more serious consequences were brought by the actions of an aggressively-minded neighboring state, which launched a hybrid war against Ukraine. Now this war waged by Russia is aimed not only at Ukraine, but at the whole world, and, therefore, the entire world community must fight the enemy.

As for Ukraine, with the start of a full-scale invasion of Russia on February 24, 2022, the number of cyber-attacks has increased significantly. Although this year they began against the Ukrainian state on the night of January 13-14, when, as a result of the actions of hackers, some government websites were hacked, in particular, web resources of the Ministry of Education, the Ministry of Foreign Affairs, as well as the Diya service. The attackers used WhisperGate software, which can destroy data.

A month later, on February 15, a huge DDoS attack took place against the websites of the Ministry of Defense, the Ministry of Internal Affairs, and several Ukrainian banks, including Oschadbank, the instigator of which was Russia, which the US presidential administration is sure of (Cyber-attacks on Ukrainian web resources..., 2022). There were several attacks between February 20-23, 2022, and already on February 27, the Ministry of Digital Transformation called on everyone to join the IT army to deter the enemy's attack on our state (This is the world's first cyber war..., 2022). And since then, the number of attacks has been growing - both cybernetic and «physical» - using missiles and weapons prohibited by the Geneva conventions.

In November 2022, the head of the Cybersecurity Department of the Security Service of Ukraine, I. Vityuk, reported that the Russian Federation was accompanying its missile strikes against Ukraine's energy facilities with the strongest cyber attacks to arrange the maximum «blackout» in the defending country. He also noted that the majority of cyber-attacks are not reported to the public, although the enemy carries out an average of more than 10 of them in the cybernetic domain of Ukraine per day. This can have a very serious negative impact since such cyber attacks can be more effective than rocket raids because a «simultaneous attack on all regional energy systems can turn off the power throughout the country.» Also, according to him, about 90% of all cyber-attacks come from Russia, and another part is carried out by the Belarusian special services for the benefit of the Russian Federation. I. Vityuk noted that about 800 cyber attacks were recorded 2 years ago, about 1,400 a year later, and in the current 2022, as of November, this number has increased to more than 3,500 (Russia daily carries out more than 10 cyber..., 2022).

All this confirms the need to maintain the high-quality functioning of cyberspace in the country. In connection with the above, it is important to understand the essence of this term, its features, technical structure, and how this issue is settled at the legal level today. A scientific understanding of the sense of cyberspace will allow for a deeper analysis of cyber incidents in it, manage it and ensure cybersecurity more carefully. This scientific work is dedicated to the issue mentioned. It should be noted that there are still few comprehensive studies on this subject matter since the topic is very new for our state. But there are detailed analyzes and studies on the topic of certain categories and issues of the information and cybernetic spheres.

So, V. M. Furashev explored the essence of cyberspace and information space and gave on their basis a definition of the concepts of "cybersecurity", "information security" and the differences between these spaces and concepts. Thus, he perceives the cybernetic

domain as a form of coexistence of a collection of material and non-material objects and methods aimed at developing, perceiving, processing, exchanging, remembering data (Furashev, 2012). T. S. Smovzhenko, Z. E. Skrynnyk, and others described in detail the features of the existence of an information-global social reality, functioning in real-time, as one that turns humanity into an integral system of worldwide communications. They analyzed and voiced the principles of information policy on the way of the development of the information society in Ukraine, and also studied in detail the information space, of which the cybernetic space is a part (Smovzhenko & Skrynnyk, 2015).

V. L. Girich and V. N. Chuprina studied the role of information and communication technologies in the life of the world community and the nature of the global information space as a bunch of information resources and infrastructures that make up state and interstate computer webs and other cross-border data transmission channels (Girich & Chuprina, 2007). The policy of the modern state, formed under the influence of the global information space, was analyzed by O. Proskurina, she also learned the main directions that state institutions and political organizations seek to comply with while integrating into the global information space. The scientist also focuses in her research on the features of the information strategy of Ukraine in the modern geopolitical space (Proskurina, 2009). I. M. Sopilko defined the concept of information security and gave a qualitative description of this phenomenon in the framework of information warfare.

As for foreign studies of this problem, Weiss M. and Biermann F. described 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). C. Gao and others qualitatively and comprehensively studied the relationship between cyberspace and real space, assessed the situational state of cyberspace, pointed out the role of network event propagation and traceability analysis, and situational modeling of cyber events to predict risks in cyberspace. They also provided a very clear definition and understanding of cybernetic geography (Guo et al., 2019).

B. P. Medeiros and L. R. Goldoni consider cyberspace as a strategic area for international relations and offer their developments in the form of an analytical tool called «The Fundamental Conceptual Trinity of Cyberspace» in the face of such characteristics of the cybernetic domain as deterritoriality, a plurality of actors and uncertainty (Medeiros & Goldoni, 2020). D.B. Hollis pays special attention to the technical architecture that ensures the functioning of the global Internet and governance in cyberspace and also points to the role of international law in cyberspace (A brief primer on international law and cyberspace, 2021). T. C. Folsom defines cyberspace as an exemplified switched network for the movement of data traffic, further characterized by degrees of admission, navigation, information action, development (and trust), and also suggests improvements in legislation to better respond to new technological challenges (Folsom, 2007).

2. Materials and Methods

This scientific article was written by a group of authors taking into account the provisions of the current Ukrainian legislation and normative regulations of other countries, as well as technical standards adopted in the information technology field. The methodological basis in 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. Thus, the dialectical method of scientific knowledge of the phenomena of reality in their relationship and development became the basis for working on this scientific article. The authors applied the empirical method in the face of describing the essence of the cybernetic space (domain) and the theoretical method in the form of analysis, abstraction, deduction, generalization, explanation, and others. The system method was also used, which helped researchers to establish a connection

between cyberspace and information space, between cybersecurity and information security, and other related categories and concepts.

Special research methods made it possible to study the unique properties characteristic of cybernetic space. Thus, the formal-logical method made it achievable to significantly deepen the conceptual apparatus of the study. The usage of the comparative legal method used by the authors made it possible to clarify the problematic issues of law enforcement in the field of ensuring the normative regulation of the functioning of cyberspace in Ukraine and providing cybersecurity and information security in the country. The method of classification and grouping was useful in the process of determining the subject-object composition of the concept of cybernetic space and related categories. The modeling method has become the basis for the development of recommendations and suggestions for improving legislation in the field of ensuring an appropriate level of cybersecurity and information security, as well as the functioning of cyberspace in Ukraine.

3. Results and Discussion

The term «cyberspace» came to us from science fiction and has become common today among technical workers, security professionals, military, state authorities, and other information subjects. It usually refers to some sort of global information technology environment where people communicate, do business, work, exchange information, and otherwise interact. This concept, for the most part, has become generally accepted in connection with the use of the World Wide Web. And if for some researchers cyberspace is a part of the national critical infrastructure (Weiss & Biermann, 2021), then for others it is a phenomenon determined not so much by technical implementation, but by social interaction (Morningstar & Farmer, 2003). Despite there are much more approaches to understanding and implementing cyberspace, which will be discussed further.

But first, it is worth noting that at the arch of the present and past centuries, both in the social and technical sciences, the term “global information space” arose and took root, which is directly related to the cybernetic space. 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. Furthermore, in connection with this term, the more narrowly focused term «global cyberspace» is often used.

So, there are several approaches to defining and understanding cyberspace. And we will directly consider them together with related categories and phenomena.

The very name of such a concept was formed from two words - «cybernetics» and «space». For the first time the term «cyberspace» «lit up» in 1984 in the book «Neuromancer» by W. Gibson. The author himself strongly criticized this concept, considering it to be somewhat «meaningless», nevertheless, the term has taken hold and is now used in all corners of the globe to describe objects and functions related to the worldwide global network. Gibson understood cyberspace as a kind of concerted illusion that a huge number of users on earth experience every day (Gibson, 2004).

From a technical point of view, it is worth paying attention to the approach of D. Hollis, who understands the concept under discussion as the technical architecture that assures the functioning of the Internet as a worldwide global network (A brief primer on international law and cyberspace, 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 (Cyberspace Definition, 2022). Also, 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», by which is comprehended the worldwide telecommunications network including computers connected to it related to state, commercial and private entities (Definition of cyberspace, 2022).

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 (What Does Cyberspace Mean, 2022). T. 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. The author mentioned 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 together constitute an objective cybernetic space with matters that can arise from its goals (Folsom, 2007).

B.P. Medeiros and L.R. 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, although it is partially divorced from physical components. The uniqueness of cyberspace as a domain lies in the fact that, unlike the three «physical» ones, it was created by people (Medeiros & Goldoni, 2020).

From the point of view of this scientific research, it is also important to know the definition of cybernetic space given by V.M. Furashev, as a form of coexistence of a special bunch of material and non-material objects, phenomena, methods, strategies the objective of which is interaction with information, that is, the creation, braining, processing of such information and knowledge, their mutual exchange (Furashev, 2012).

Accordingly, we can conclude that there is no single unified and standardized definition of the term «cyberspace». One thing is clear that in all approaches to its understanding, we are necessarily talking about a system of connected computers, digital networks, and other communication and information technologies. Thus, 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, and the like. Looking ahead, we note that cyberspace also includes the worldwide Internet, which we will discuss further.

The possibility of using the term «cyberspace» in a purely practical plane is evidenced both by its mention in many sources of scientific literature and by its official fixing in the legislation of numerous countries. So, concerning international legal documents, 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. And it is essential to do this 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 the latest regulatory document, the concept in question was represented as an interconnected network information infrastructure, the components of which are telecommunication networks, as well as various systems and embedded processors and controllers used in critical industries (Lieberman, 2010). But this is local regulation.

It is also worth considering the standards for software solutions of the National Institute of Standards and Technology (also NIST) and the American National Standards Institute (also ANSI) (Supplemental Information for the Interagency Report..., 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 in its structure, that is, computer systems, embedded processors and controllers in critical industries, as well as telecommunications networks and the Internet directly (Guide for Conducting Risk Assessments, 2011; Managing Information Security Risk. Organization, Mission, and Information System View, 2011; Security and Privacy Controls for Federal Information Systems and Organizations, 2021). But 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 (Developing Cyber-Resilient Systems..., 2021).

Summing up the information on the issue of international legal support of cyberspace, we can say that current international law does not contain special norms and rules for regulating relations in it. In this regard, D. Hollis points to some understatement and insufficient regulation regarding the application of the norms of the current international law to cyberspace, although some international actors such as the Group of Twenty, the First Committee of the UN General Assembly on Disarmament and International Security, the EU and others have already revealed their agreement with the applicability of international law in interaction with information and communication technologies. That is, the question rather concerns not the possibility of applying international law, but how this will be done (A brief primer on international law and cyberspace, 2021).

It should be understood that 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. But such advantages come with some challenges. Accordingly, the special intangible nature of the studied space significantly complicated not only the definition of such a phenomenon itself but also the substantiation of its legal foundations with their subsequent normative consolidation in official state sources. In this regard, we note that the national legislation of Ukraine concerning cyberspace is represented, first of all, by Law 2163-VIII On the Basic Principles for Ensuring Cybersecurity of Ukraine dated October 05, 2017. This normative act regulates the basis for ensuring the protection of the country's national interests in cyberspace, as well as the vital interests of the main subjects of the relevant relations - an individual and a citizen, society and the state. Its action also extends to the key goals and directions of state policy, the powers, and principles of coordination of the activities of state bodies, institutions, and other entities to ensure cybersecurity. Article 1 (paragraph 11) of Law 2163-VIII defines cyberspace as a virtual domain created as a result of the operation of connected, compatible communication systems and electronic communications using the World Wide Web, as well as, if necessary, other global information transmission networks. Such a space allows everyone to communicate and execute social relations in it (On the main principles of ensuring the cybersecurity of Ukraine, 2022). Cyberspace is thus an ever-evolving environment that changes as technology advances and adapts to new emerging user needs. We are talking about a unique domain, because, unlike the already existing land, water, and air spaces, the cybernetic was created by people. And, due to the ongoing technological research and increasing user experience, it is characterized by constant variability. We also should mention the important «information» component of cyberspace. So, it is distinguished by the absence of geographic reference, as well as the boundaries of physical space. This shows its transboundary character. But also the cybernetic domain does not exist on its own, it is inextricably linked with the information sphere (environment). For this scientific study, it is also important to understand the essence of the last concept. For this, we turn to 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, which says of one of the main priorities of the Ukrainian state - the desire to form 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, and the like. Through this, every Ukrainian will be able to fully realize his potential, which will not only improve the quality of human life but will allow him to develop, as well as the society as a whole (On the Basic principles for the development..., 2007). The organizational

and legal foundations for the development of the information society in Ukraine are considered in paragraph 3 of Section IV of Law No. 537-V, which include resource, institutional, and integration. To achieve the latter, namely, to integrate the Ukrainian state into the global information space, it is important that Ukraine actively participate in the latter, as well as to conduct active international cooperation on reducing the digital and information divide between subjects and implementing a universal general active approach. To achieve these objectives, in addition to expanding the sphere of influence and cooperation with major international actors, the Law under consideration 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). Also, 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 the Law No. 2657-XII «On Information» dated October 02, 1992 (On information, 2022).

If we recall the previously mentioned global information space, we can consider it as an important element of the social space, even as a kind of special «social information space». As O. Proskurina comments, in the course of implementing the information strategy, an important direction for Ukraine should be precisely the active participation in the work of international actors aimed at the political and legal regulation of the global information space. In this regard, Ukraine should join international treaties on the procedure for the activities of official and non-official bodies in information networks (Proskurina, 2009). 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. The mentioned resources, in turn, are websites, various texts, databases, and other content. It is these resources in their totality that form a single information space through the information and communication infrastructure (Girich & Chuprina, 2007).

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

- a sphere of subjective activity where data are produced, consumed, altered;
- a similar sphere of subject activity within the framework of public life, which, in addition to the already indicated actions, also includes the preservation of information, its dissemination, and processing;
- the plurality of the knowledge and information themselves, the information infrastructure, and the subjects carrying out information activities;
- a set of systems of information resources, the interaction of information, as well as 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. But, as in the case of cyberspace, information has no physical boundaries but has an objective virtual component.

To summarize the above, we can say that the terms «cyberspace» and «information space» are not identical, although they are very similar. So, they differ primarily in their focus. Accordingly, if we mean cybernetic space, then it is an inseparable element of the information space, covering only living beings that perceive, process, recall data, and exchange acquired knowledge. And the information space (information environment)

applies to all sources of information in general, while the subjects of interaction are not required to appropriately perceive data, exchange them, process them, and so on.

At the same time, according to V. M. Furashev, both of the categories under consideration 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). And yet, cyberspace and information space are different concepts. And, in our opinion, the first should be considered as an element of the system of the second, and not just as an element, but as an important segment in which global flows of both an economic and political character and social relationships are concentrated.

Now let's discuss the important characteristics of cyberspace - deterritoriality, multiple actors, and uncertainty. As sure B.P. Medeiros and L.R. Goldoni, each of these characteristics do not pose a problem, but when they work together, and when operated by users for their purposes, issues can arise. In this regard, we note that, unlike traditional spaces, cybernetic, as mentioned earlier, is not limited by territorial boundaries. It is essentially intangible, yet dependent on mobile devices operating in traditional spaces. It is possible to conclude the simultaneous «presence» of cybernetic space in the other three through the information flows of the electromagnetic spectrum. The deterritorializing nature of the phenomenon under consideration is manifested in its partial non-materiality, but such a space is both an object and a means of power relations. And when the relevant subjects use it and the opportunities provided by it, for their selfish purposes, the territorialization of cyberspace occurs. In this regard, some difficulties arise in the form of challenges to 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. To it undoubtedly contribute wide prevalence and low costs of use (Medeiros & Goldoni, 2020).

This multiplicity resulted in an opportunity for intelligence agencies to track the conversations of the tops of state power, businessmen, and researchers in all corners of the planet, and now terrorists can recruit dissidents from other lands without any problems; hackers can cause significant physical damage to the critical infrastructure of the state and the like. The low cost of use allows cybercriminals to easily and at minimal cost commit sabotage in the cybernetic domain, for example, against a specific airport, as was the case with Ukraine in 2017 due to the Petya virus, than to train people, acquire and operate special equipment to destabilize the work of the airport. Everything 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, and this undermines accountability processes. As a result, there is a lack of indicators of success and anonymity and the very uncertainty of cyberspace. Concerning the issue of accountability, note that such a thing results in the form of speculation in an international context. In this case, 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).

Further, we will analyze in more detail the main sources of Ukrainian legislation related to the topic of this study. Earlier, the main Ukrainian legal document that regulates issues related to cyberspace has already been mentioned, this is Law No. 2163-VIII, better known as the Law on Cybersecurity. It has not only defined cyberspace, but also cybersecurity itself. The latter, according to paragraph 5 of Article 1 of this Law, 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. It is under this condition that not only the sustainable development of the Ukrainian information society, but also the digital communication environment is ensured, and it also provides the identification, precluding, and elimination of possible or real threats to the national security of the Ukrainian state in cybernetic space (On the main principles of ensuring the cybersecurity of Ukraine, 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. The latter is of particular interest in the context of this scientific study.

Information security can be defined as a special state of protection of the information environment of the Ukrainian society, in which information subjects represented by the mentioned society, its members, and the state as a whole can freely develop information, and also have complete confidence 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 info provided, as well as no its integrity, confidentiality and availability are violated (On the Basic principles for the development..., 2007). Because of the foregoing, we conclude that cybersecurity is an important element of information security, which in turn is a pivotal segment of national security.

In addition to Law No. 2163-VIII on Cybersecurity, the regulation of the cyber domain in Ukraine is governed by several other legal instruments, including:

- The Ukrainian Constitution of 1996;
- Various laws, such as the «On Information» Law (dated October 2, 1992, No. 2657-XII), the «On the Fundamentals of Domestic and Foreign Policy» Law (dated July 1, 2010, No. 2017), the «On the National Security of Ukraine» Law (dated June 21, 2018, No. 2469-VIII), and the «On Electronic Communications» Law (dated December 16, 2020, No. 1089-IX);
- International treaties ratified by Ukraine, in accordance with Article 9 of the Constitution, and approved by the Verkhovna Rada;
- Decrees issued by the President of Ukraine;
- Regulations established by the Cabinet of Ministers of Ukraine;
- Other relevant 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 arrows for solving tasks mentioned to achieve a suitable level of protection of the cyberspace of the state. In addition to the noted legal instruments, a bunch of principles should also be suggested, without which, in our opinion, it will be challenging to achieve these objectives using only the application of the norms of the existing legal framework. These are the principles of:

- respect for human rights and freedoms. After all, as O. Mironets appropriately notes, the prevention of human rights violations is an essential element of the defensive policy of each state (Myronets et al., 2019). According to this fundamental, all activities of the authorities in cybernetic space should be aimed at providing the observance of such rights and interests, and any limitations imposed should not violate them;
- responsibility. Each player in a cybernetic domain must be responsible for preserving stability in it;
- rationality and cognition. Each participant of relations in the space mentioned must assume before acting in such a way that it could 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 bodies ensuring the functioning of the cybernetic space in Ukraine.

Equally noteworthy, we consider the development and undertaking of guides and standards aimed at preventing destabilizing actions, as well as at stimulating the implementation of steps to intensify the stability of cyberspace.

4. Conclusions

With the help of a bibliographic review and legal analysis in this scientific paper, an attempt was made to define cyberspace, conceptualize it, and determine its distinctive technical, social, legal components. This, first of all, will help develop new and improve existing local legislation, as well as promote a holistic and strategically oriented understanding of the role of the 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 domain under consideration. Although cyberspace is, nonetheless, a more multifaceted phenomenon that harmoniously combines resource, technical, 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.

It can be concluded that today, to build a full-fledged and comprehensive legal support for the functioning of cyberspace in Ukraine, as well as maintaining the national information security at the proper level in the country, the following is required:

- strengthening and continuous improvement of the national cyber and information security system with the involvement of not only government agencies, but also the active public, 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 ownership rights to them, 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. Our society is an information one, and, therefore, the protection of data with limited access in the conditions of its existence is impossible without the development and implementation of a flexible legal framework and a balanced state policy in the infosphere;
- all favoring digitalization and the outgrowth of information technology potential, the development of a competitive Ukrainian information product;
- formation and provision of information and psychological safety of information subjects. In connection with the development of information technology, today we are witnessing the dominance of fake data and other misinformation. Consequently, it is important to protect the consciousness of both individuals and the entire society from negative information impact, for which, among other things, it is important to teach Ukrainians cyber and information hygiene;
- providing worthy counteraction to cybercriminals and cyberterrorists. For the work of almost every sector of the economy and other areas of social interaction, information and telecommunication technologies cannot be dispensed with, and therefore they must be reliably protected from the actions of intruders;
- formation and promotion of a positive image of our state on the Internet as one that in every possible way supports and helps to develop the information society.

We are confident that by ensuring the achievement of these objectives, Ukraine will be able to become a worthy member of the global information space, and directly cyberspace based on equality and independence.

References

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

- 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>
- Cyber-attacks on Ukrainian web resources are possible on February 22 – CERT-UA (2022). *Ukrainska Pravda*. Retrieved from: <https://www.epravda.com.ua/rus/news/2022/02/21/682554/>
- Cyberspace Definition (2022). *Duhaime Legal Dictionary*. Retrieved from: <https://www.duhaime.org/legal-dictionary/term/cyberspace>
- Definition of cyberspace (2022). *TheFreeDictionary*. Retrieved from: <https://legal-dictionary.thefreedictionary.com/cyberspace>
- 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>
- 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
- Guide for Conducting Risk Assessments (2011). *NIST 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>
- 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>
- Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid (2016). *WIRED*. Retrieved from: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>
- 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>
- 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>
- 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>
- Morningstar, C. & Farmer, F. R. (2003). The Lessons of Lucasfilm's Habitat. In: *The New Media Reader* (pp. 664-667). London: The MIT Press. Retrieved from: https://monoskop.org/images/4/4c/Wardrip-Fruin_Noah_Montfort_Nick_ed_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.
- On information (2022). *Law of Ukraine No. 2657-XII*. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2657-12#text>
- 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>
- On the main principles of ensuring the cybersecurity of Ukraine (2022). *Law of Ukraine*

- of No. 2163-VIII. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2163-19#text>
- 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
- Russia daily carries out more than 10 cyber-attacks on strategic objects of Ukraine – SSU (2022). *Ukrainska Pravda*. Retrieved from: <https://www.pravda.com.ua/rus/news/2022/11/9/7375609/>
- Security and Privacy Controls for Federal Information Systems and Organizations (2021). *NIST Special Publication 800-53 Revision. 5*. Retrieved from: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf>
- 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>.
- Supplemental Information for the Interagency Report on Strategic U. S. Government Engagement in International Standardization to Achieve U. S. (2015). *NISTIR 8074*. Retrieved from: <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf>
- This is the world's first cyber war. The Ministry of Digital told about the Ukrainian IT army (2022). *Suspilne News*. Retrieved from: <https://suspilne.media/222186-ce-persa-u-sviti-kibervijna-u-mincifri-rozpovili-pro-ukrainsku-it-armiu/>
- 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>
- What Does Cyberspace Mean? (2022) *Techopedia*. Retrieved from: <https://www.techopedia.com/definition/2493/cyberspace>