CYBERSECURITY AS A COMPONENT OF INTERNATIONAL SECURITY

[a]OLEKSANDR HOMANIUK

[a]Lesya Ukrainka Volyn National University, 13, Voli Ave, 43025, Lutsk, Ukraine
email: [a]alex.ua.man@gmail.com

Abstract: This article examines cybersecurity issues in the modern world, where information technologies play a critical role in political, economic, and military spheres. The growth of digital infrastructure is accompanied by an increase in cyber threats, which can be directed against both individual states and the international community. The article emphasizes that cybersecurity is becoming a critically important aspect of both national and international security, requiring collective efforts to protect against potential threats such as cyberattacks on government institutions, critical infrastructure, as well as espionage and social engineering. Special attention is given to analyzing various forms of cyber threats and their impact on global security. Specific examples of cyberattacks are described, including interference in the U.S. election processes and attacks on Ukraine's energy infrastructure. The authors highlight key aspects of cybersecurity, including technical, legal, and educational measures aimed at ensuring security in the digital space. The article also addresses the role of international cooperation in the context of cybersecurity, emphasizing the importance of joint efforts by governments, the private sector, and international organizations such as the UN, NATO, and the EU. The strategies of various countries, including the U.S. and Israel, in the field of cyber defense, as well as steps taken by Ukraine to strengthen its cybersecurity amid Russian aggression, are also reviewed. The article discusses the challenges related to cybersecurity, including insufficient funding, the rapid pace of technological advancement, the human factor, and the absence of unified international legal frameworks in cyberspace. The article underscores the need for the development of national cybersecurity strategies and close cooperation among states to counter the growing cyber threats in a globalized world.

Keywords: cybersecurity, cyberattacks, cyber threats, information security, critical infrastructure, hybrid warfare, international cooperation, national security, digital infrastructure.

1 Introduction

In the modern world, information technologies play a key role in all areas of life, including the economy, politics, military operations, and interpersonal communications. As digital infrastructure evolves, the number of cyber threats that endanger both individual states and the international community as a whole continues to grow. Cybersecurity has become one of the critical components of both national and international security, requiring collective efforts for its provision. This issue encompasses various aspects, from protecting critical infrastructure to preventing global cyberattacks capable of destabilizing the geopolitical landscape. It is not only a technological issue but also a geopolitical one, as threats can originate from individual hackers or state actors. Given the rise of hybrid warfare, cyberattacks, and information campaigns actively used as tools of influence, the protection of national interests in cyberspace has become one of the primary tasks for governments. For Ukraine, which has long been subjected to military aggression from the Russian Federation, cybersecurity is a crucial component of national security, particularly in light of the large-scale cyberattacks accompanying military actions. Despite the declared intentions of major geopolitical actors to counter the militarization of cyberspace, the increasing role of purely military structures in ensuring the security of critical national infrastructure (national cyberspace) is evident. Initiatives within the United Nations to develop comprehensive approaches to international information security are likely to either fail completely or achieve limited success (in the form of declarative agreements). In such conditions, Ukraine must be prepared not only for defensive cyber warfare but also for actively developing its own offensive capabilities in cyberspace. The aim of the study is to analyze modern cyber threats, particularly in the area of protecting the state's critical infrastructure, and to determine the role of international cooperation in countering cyberattacks and hybrid threats. The research focuses on how to effectively strengthen information security and increase resilience to cyberattacks in a globalized digital environment.

2 Materials and Methods

Document analysis – the study of legislative acts, international agreements, and cybersecurity strategies; comparative analysis – a comparison of cybersecurity approaches in different countries; case study method – analysis of specific examples of successful and unsuccessful cyber defense operations and attacks; empirical research – the collection and analysis of data on current cyber threats and incidents; content analysis – the examination of media reports and information campaigns in the context of hybrid warfare. These methods provide a comprehensive assessment of both the current state of cyber threats and the necessary measures to address them.

3 Results and Discussion

Cybersecurity is defined as a set of measures aimed at protecting information systems, computer networks, and data from unauthorized access, attacks, destruction, and misuse. It encompasses technical, organizational, legal, and educational aspects, all designed to ensure the uninterrupted and secure operation of systems. The importance of cybersecurity grows in direct proportion to the level of digitalization in society and its reliance on information technologies.

According to the ISO/IEC 27032:2012 standard, cybersecurity or cyberspace security refers to the preservation of the integrity, confidentiality, and availability of information circulating within a cyber system (i.e., information entering, accumulating, and being stored in the cyber system for further processing) to ensure the resilience and continuity of the system's management functions over relevant objects of control [12]. Correspondingly, cyberspace is the part of the information space formed by information flows and fields generated during the operation of cyber systems [9].

In a world where financial systems, government institutions, energy infrastructure, military networks, and even household technologies depend on the Internet, any vulnerabilities can have global consequences. According to various studies, cyberattacks cause annual losses in the trillions of dollars and have the potential to destabilize national economies, undermine trust in governments and corporate structures, and result in human casualties in the event of attacks on critical infrastructure.

Cyber threats take various forms and can target different entities. Among the most common threats are [13]:

- Cyberattacks on government institutions. These include attempts to steal information, breach national security systems, or influence political processes, such as elections. A notable example is the interference in the 2016 U.S. elections, where hackers sought to affect the election outcome.
- Attacks on critical infrastructure. Energy systems, water supplies, transportation networks, and other essential services may be targeted in cyberattacks, leading to catastrophic consequences. The 2015 attack on Ukraine's energy system was one of the first examples of a cyberattack on critical infrastructure.
- Malware and viruses. Malicious software, such as viruses, Trojans, and ransomware, can be used to steal data, damage systems, or extort money. For example, the WannaCry virus in 2017 locked computers worldwide, demanding a ransom for their release.
- Cyber espionage. States may use cyber tools to spy on other nations or steal classified information, potentially escalating international conflicts.
- Social engineering and phishing. These techniques exploit psychological manipulation to trick users into revealing confidential information or downloading malicious software.

Today, many countries have integrated cybersecurity as an essential part of their national security strategies. Governments are establishing specialized agencies and centers focused on cybersecurity, developing relevant legislation, and supporting the growth of necessary infrastructure. For example, in the

United States, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for protecting both public and private entities from cyber threats. In the European Union, the European Union Agency for Cybersecurity (ENISA) assists member states in coordinating their cybersecurity efforts.

Many nations are also incorporating cybersecurity into their military strategies. Cyberspace is now considered the fifth domain of warfare, alongside land, sea, air, and space. Military cyber divisions are engaged in both defending their own systems and developing offensive cyberattack capabilities. This includes the potential to disable enemy command, communication, energy, and other critical infrastructure systems.

Threats in cyberspace are becoming increasingly complex and diverse. The primary threats include:

- Cyber espionage. The use of cyber tools to gather information on government, military, and economic structures of other states can pose a serious threat to national security. Stolen information can be used to influence internal and external political processes.
- Cyberterrorism. Hackers may target a country's critical infrastructure, such as power plants, water supply systems, and transportation networks, potentially leading to mass disasters and destabilization.
- Cyber warfare. In modern military conflicts, cyber weapons are used alongside traditional military means. States are developing cyber military units to conduct offensive and defensive operations in cyberspace.
- Destabilization of the information space. Fake news, disinformation, and propaganda can disrupt political stability and undermine trust in government institutions, directly impacting national security.

Cyberattacks targeting Ukraine share common characteristics: Russian intelligence services actively employ cyber tools to gather information on political, military, and economic processes in Ukraine. These attacks aim to acquire strategic information and use it to destabilize the situation. As demonstrated by attacks on energy systems, cyberattacks can paralyze critical infrastructure, causing significant harm to the country's economy and security. Cyberattacks are often accompanied by information operations designed to undermine trust in Ukrainian institutions, create panic, or influence public opinion. Given that many strategically important infrastructures are privately owned, attacks on companies represent another form of cyber threat [7].

International cybersecurity cannot be achieved without close cooperation between states, as cyberattacks transcend borders. The Internet is global, and attacks launched from one country can cause harm in others. Therefore, international collaboration is crucial to developing effective mechanisms to counter cyber threats.

Organizations like the United Nations, NATO, the European Union, and others are actively developing standards, policies, and strategies in the field of cybersecurity. For example, within NATO, cyber defense is one of the top priorities for collective security, and a cyberattack may be considered grounds for invoking Article 5 of the NATO Charter, which calls for collective defense. The UN hosts conferences and consultations aimed at establishing global rules and norms for state behavior in cyberspace. Efforts to create an international code of conduct in cyberspace are focused on limiting the use of cyber tools for military purposes and ensuring the stability of the digital space.

Despite all efforts, cybersecurity remains a significant challenge for the international community. A critical issue is the lack of unified international rules and norms in cyberspace. Many states utilize cyber tools to achieve their own geopolitical objectives, leading to conflicts and tensions on the global stage.

Another important aspect is technological progress. With the emergence of new technologies such as artificial intelligence, quantum computing, and the Internet of Things, the possibilities for cyberattacks are also increasing. Protecting against these threats requires constant improvement of cybersecurity systems and enhancing the training of specialists in this field.

Various countries are developing their approaches to cybersecurity, yet common features exist in the formation of strategies. The American cybersecurity strategy focuses on protecting critical infrastructure, developing offensive cyber capabilities, and fostering active international cooperation. The United States is also investing significantly in artificial intelligence and quantum computing technologies to enhance cybersecurity.

Israel is regarded as one of the world leaders in cybersecurity, due to intensive collaboration between the government, private sector, and universities. The Israeli cyber forces are recognized as some of the most effective in the world, and the country actively develops the export of cybersecurity technologies. In 2013, the European Union adopted the Cybersecurity Strategy, aimed at creating an open, reliable, and secure cyberspace. This includes measures in various areas: achieving cybersecurity resilience, significantly reducing cybercrime, developing a cyber defense policy related to the Common Security and Defense Policy, enhancing manufacturing and technological resources for cybersecurity, creating a coordinated international cyber policy for the EU, and promoting the core values of the EU [4].

The analysis of trends in the European Union's cybersecurity policy indicates that the development of digital technologies and information systems has led to new threats to the national security of European countries. Modern information technologies render information systems vulnerable to cyberattacks, necessitating measures to mitigate the negative impacts of these threats [2; 14].

The European Union is actively working to enhance its cybersecurity systems in response to contemporary challenges. This includes streamlining the regulatory framework, developing European principles for Internet resilience, increasing the number of divisions focused on cybersecurity, strengthening control over the national information space, and protecting critical infrastructure. Additionally, pan-European exercises and studies on security incidents in cyberspace are being conducted [3; 5; 8].

The European Union is continually updating its cybersecurity sectors to address modern challenges. This process encompasses the following: organizing the regulatory framework that ensures the integrity of state policy in this area; developing European guidelines to ensure Internet resilience and promoting them internationally; increasing the number of units involved in the cybersecurity system; enhancing oversight of the national information space; strengthening protective mechanisms for the EU's critical information infrastructure; conducting Europe-wide training and research on Internet security incidents; strengthening collaboration between the public and private sectors; establishing a European forum for information exchange among member states; and creating a European early warning system for cyber threats, among others [1].

For Ukraine, it is crucial to become an active participant in these processes, as this will not only enhance its international image but also influence the formation of the organizational and legal foundations of national cybersecurity[10]. In the context of hybrid warfare, cybersecurity issues must be at the center of state policy. Ukraine's foreign policy strategy in the field of cybersecurity should clearly define its goals and methods for achieving them, to foster beneficial partnerships with the EU in safeguarding national interests.

Ukraine requires the establishment of an adequate security system in a transforming world, where national security challenges increasingly exhibit characteristics distinct from traditional threats. The activity of leading states in cyberspace, profound changes in the approach to domestic information policy, and the formation of powerful transnational criminal groups specializing in cybercrimes all underscore the necessity

to develop recommendations for the short- and long-term priorities for transforming the national security sector in light of these trends [7].

Since the onset of Russian aggression in 2014, Ukraine has faced a series of powerful cyberattacks, prompting the government to reassess its approaches to cybersecurity. The world's first documented case of a successful hacker attack on energy infrastructure occurred on December 23, 2015, in Ukraine. As a result, automated control systems for energy substations were incapacitated, leading to power outages lasting from 3 to 8 hours. The incident was reported by Kyivenergo, Prykarpattyaoblenergo, and Chernivtsioblenergo [13]. New structures have been established in the country, such as the National Cybersecurity Coordination Center, and cooperation with international organizations, such as NATO and the EU, has been strengthened.

In the context of cybersecurity, close interaction between the government and the private sector is crucial, as many critical infrastructures, such as banks, telecommunications, and energy, are privately owned. Government agencies must ensure the establishment of regulatory frameworks that allow companies to effectively protect their information resources, as well as promote the sharing of information about potential threats. The private sector plays a key role in developing new protection technologies and in implementing security standards. Investments in cybersecurity enable companies to reduce the risks of cyberattacks, maintain data confidentiality, and protect their reputation.

The implementation of national cybersecurity strategies faces a number of challenges:

- Insufficient funding: In many countries, investments in cybersecurity remain inadequate, hindering the development of the necessary infrastructure and the training of specialists.
- Rapid pace of technological progress: The emergence of new technologies, such as artificial intelligence, quantum computing, and the Internet of Things, creates new threats that states may not be prepared to address.
- The human factor: Even the most advanced protection technologies can be ineffective if users make mistakes. Training and raising awareness among public officials and citizens remain critical aspects of ensuring cybersecurity.
- International law and its absence: Currently, there are no unified international legal frameworks to combat cyberattacks. This complicates cooperation among states and creates loopholes for cybercriminals who can operate from one country without facing prosecution from another.

The Law of Ukraine “On the Fundamentals of Ensuring Cybersecurity in Ukraine” established the overall architecture of the national cybersecurity system and delineated tasks and authorities among the main entities responsible for cybersecurity, including the National Cybersecurity Coordination Center, the Ministry of Defense, the General Staff of the Armed Forces, the State Special Communications and Information Protection Service, the Security Service of Ukraine, the National Police, the National Bank, and the intelligence agencies of Ukraine [11]. In response to cyber threats, Ukraine developed the National Cybersecurity Strategy, which outlines priorities and measures to strengthen cyber protection. The main elements of this strategy include:

- Strengthening the regulatory framework: A significant step was the adoption of the Law "On the Fundamentals of Ensuring Cybersecurity in Ukraine," which defines the primary directions of state activity in the field of cybersecurity. Additionally, the National Cybersecurity Coordination Center was established under the National Security and Defense Council of Ukraine.
- Developing institutional infrastructure: Ukraine is creating specialized cybersecurity units at both military and civilian levels. These bodies are engaged in monitoring cyber threats, analyzing data, and developing operational response measures to cyberattacks.
- International cooperation: Ukraine actively collaborates with international partners, particularly with the EU and NATO, in the area of information exchange regarding cyberattacks and the development of joint cybersecurity mechanisms. This cooperation allows Ukraine to obtain the necessary technologies and expertise to strengthen its own cyber environment.
- Protection of critical infrastructure: Ukraine is enhancing measures to protect critical infrastructure, such as energy, transportation, and financial systems. This includes both strengthening physical security and implementing modern cybersecurity technologies.
- Educational programs and workforce training: An essential component of the strategy is the training of specialists in the field of cybersecurity. Ukrainian universities are developing specialized educational programs to prepare a new generation of cybersecurity professionals for both the public and private sectors.

4 Conclusion

Cybersecurity is a crucial component of modern international security as cyber threats can have global repercussions. Effectively addressing cybersecurity issues requires international cooperation, harmonization of legislation, the development of new protective technologies, and the continuous improvement of strategies. States and international organizations must intensify their efforts to create a secure and stable cyberspace, which will serve as the foundation for global security. Ukraine’s National Security Strategy clearly defines cybersecurity as a priority area for the protection of the state [6]. Cyber threats in Ukraine are not hypothetical—since 2014, the country has been the target of large-scale cyberattacks on key state, military, and energy facilities. Thus, cybersecurity for Ukraine is not only about protecting information infrastructure but also about the security of vital sectors. The Ukrainian government and international partners are actively working to establish a reliable cybersecurity system that will ensure the safety of government institutions, the economy, citizens, and critical infrastructure.

Literature:

1. About ENISA / European Union Agency for Network and Information Security. (n.d.). Retrieved September 10, 2024, from https://www.enisa.europa.eu/about-enisa
2. Biriets, K. Y. e. (n.d.). Cybersecurity as an important component of the national security protection system of European countries. Retrieved September 10, 2024, from 15739.pdf (vntu.edu.ua)
3. Cyber Europe / European Union Agency for Network and Information Security. (n.d.). Retrieved September 10, 2024, from https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
4. Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace. (2017). Retrieved September 10, 2024, from http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
5. Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace: Adopted by the European Commission on February 7, 2013 / European Union. (n.d.). Retrieved September 10, 2024, from https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity
6. Decree of the President of Ukraine No. 392/2020 on the decision of the National Security and Defense Council of Ukraine dated September 14, 2020, "On the National Security Strategy of Ukraine." (2020). Retrieved November 26, 2023, from https://www.president.gov.ua/documents/3922020-35037
7. Dubov, D. (n.d.). Modern trends in cybersecurity policy: Conclusions for Ukraine. Analytical note. National Institute for Strategic Studies (NISS). Retrieved September 10, 2024, from https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini

8. EU cybersecurity initiatives working towards a more secure online environment / European Union. (n.d.). Retrieved September 10, 2024, from http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf
9. Lipkan, V. A., & Lipkan, O. S. (2018). National and international security in definitions and concepts (2nd ed., revised and expanded). Kyiv: Educational Manual.
10. National Cyber Security Index. NCSI. URL: https://ncsi.ega.ee/ncsi-index/ (Retrieved November 7, 2023).
11. On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017. (2017). Bulletin of the Verkhovna Rada (VVR), No. 45, 403 p.
12. Slipchenko, T. (2020). Cybersecurity as a component of the national security protection system: European experience. Current Issues of Jurisprudence, 1(21), 128-133.
13. Yemelianov, V. M., & Bondar, H. L. (n.d.). Cybersecurity as a component of national security and cyber protection of Ukraine's critical infrastructure. Public Administration and Regional Development, (5), 493-523. Retrieved September 10, 2024, from https://doi.org/10.34132/pard2019.05.02
14. Zaporozhets, O. Yu. (2009). The European Union's policy in the field of information security. Current Issues of International Relations, 87(II), 36-45.

Primary Paper Section: A

Secondary Paper Section: AD