relevant results and theoretical developments
of science and research

14

2024
issue 1, special XLII.

AD ALTA

Journal of Interdisciplinary Research

AD ALTA: Journal of Interdisciplinary Research
Double-Blind Peer-Reviewed
Volume 14, Issue 1, Special Issue XLII., 2024
Number of regular issues per year: 2

MAGNANIMITAS Assn.

INTERNATIONAL LEGAL REGULATION OF CYBER POLICY, CYBER SECURITY, AND DIGITAL CONFLICTS: INTERNATIONAL COOPERATION OF STATES

[a]OLEKSANDR SKRYPNIUK, [b]HALYNA ZAVORITNYA, [c]ANASTASIIA CHYSTIAKOVA, [d]VOLODYMYR KOMAROV, [e]MYKHAILO KRAVCHENKO

[a]Koretsky Institute of State and Law of National Academy of Science of Ukraine, Kyiv, Ukraine.
[b]Educational and Scientific Institute of Public Administration and Civil Service of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
[c]University KROK, Kyiv, Ukraine.
[d]Military Institute of Telecommunications and Informatization named after Heroes Krut, Kyiv, Ukraine.
[e]Kyiv National Economics University named after Vadym Hetman, Kyiv, Ukraine.

email: [a]alexander.skrypniuk@gmail.com, [b]galka.zavor@knu.ua, [c]achi2021@yahoo.com, [d]vladimir@komarov.in.ua, [e]m.g.kravchenko@ukr.net

Abstract: Information can be as harmful as weapons in today's world.Cyber threats are increasing every year, making this issue more relevant than ever. Cyberattacks are chaotic activities that aim to cause harm or destruction to vital information. The purpose of the article is to examine the relationship between international law and cyberspace, specifically focusing on the legal aspects of cybersecurity and digital conflicts. The protection of the information space is a pressing issue that requires fruitful cooperation among leading countries worldwide. International cooperation in cybersecurity aims to find ways to protect against external threats by improving the regulatory and technical framework. It is important to note that the security situation in the world is increasingly threatened by cyber threats every year. Currently, countering cybercrime is mainly focused on improving international legal norms and balancing the legislation of leading countries in the world. The article discusses the importance of studying cybersecurity in modern cyberspace. It characterises the main concepts of the topic and reveals the content of international methods for combating cybersecurity. Emphasis is placed on the expediency of fruitful cooperation among leading countries in overcoming the negative impact of cyberattacks on infrastructure, economy, government, and security sectors. The importance of Ukraine's collaboration with major global powers in safeguarding the information space is highlighted.

Keywords: cyberattack, cybersecurity, digital conflict, Internet, international law, unauthorized actions with information, countering cyber-attacks, finance, financial security.

1 Introduction

The topic of cybersecurity is a prominent issue in international legal discourse. Discussions on this topic have been ongoing for decades and have yielded fruitful results. Strengthening cyberspace is not the responsibility of one state alone but requires a comprehensive approach from all developed countries. As the saying goes, “many hands make light work”. The cooperation of developed countries in the field of cybersecurity is reinforced by legal developments and outlined by strategies that must be followed. The purpose of the study is to examine the unique features of international law in relation to cyberspace, specifically focusing on cybersecurity and digital conflicts.

2 Literature review

Insufficient attention has been given to researching the peculiarities of international law and cyberspace, as well as aspects related to cybersecurity and digital conflicts in domestic practice. Some domestic scholars study this problem based on domestic experience. In international law, cybersecurity is a significant issue. In his research, M. V. Kamchatyi (2017) outlines the main principles of conducting cyber warfare in the international information space. Another researcher, Yu. H. Danyk, investigates the basics of cybersecurity and cyber defence, elucidating key concepts such as “cybersecurity”, “cyber threat”, “cyberattack”, and others. V. Ya. Novytskyi suggests that one of the main reasons for conducting cyber warfare is to influence contemporary world politics. The author describes the unique aspects of conducting cyber warfare in the current political and legal landscape.

3 Research methods

The paper employs general scientific and specific research methods. General scientific methods are used to identify the main issues of the topic, such as cyberspace, cybersecurity, and information technology. Specific methods include the systemic-structural method, which characterises the international legal mechanisms actively employed in modern international law to combat cyber threats. In general, the use of scientific and technical methods provides comprehensive coverage of international law and cyberspace issues.

4 Results

The development of science and technology has influenced the nature of collaboration among people. As non-verbal communication is the primary form of interaction, ensuring information and cybersecurity becomes particularly important in this context (Novytskyi, 2021, 85).

It is essential to note that there are currently 7.8 billion people inhabiting the planet Earth, 4.2 billion of whom are active internet users. The UN reports a steady growth in the number of new internet users. The COVID-19 pandemic in 2019 highlighted the importance of the internet for remote work, education, online sales, negotiations, business, and communication, in addition to entertainment. According to the UN's statistical data, internet traffic tripled during the pandemic period (COVID-19, 2020).

The main tasks facing state institutions include ensuring information and digital sovereignty:

- bringing legislation in line with international standards in the field of cybersecurity;
- preventing the use of advanced information technologies to disseminate harmful information that could harm society and individual groups;
- finding a socially acceptable balance between freedom of speech and the dissemination of information;
- transition of state institutions to the use of software and hardware that has several levels of protection, etc.

The significance of the Internet is widely acknowledged. Statistical data highlights the need for regulation of legal relations pertaining to its use, protection of human rights and freedoms, peaceful network usage, self-defence against cyberattacks, and safeguarding information and data confidentiality. Other issues that may arise during network usage must also be addressed. The issue of defining and establishing an international legal regime for cyberspace deserves special attention (Nihreieva, 2020).

As per Article 2, Clause 54 of the Law of Ukraine “On Electronic Communications”, the Internet is defined as a global electronic communication network designed for data transmission. It comprises logically and physically connected elements of individual communication networks, and its functioning is based on specific processes and network protocols (Law No. 1089-IX, 2020). In scientific literature, the term “cyberspace” refers to an environment created by physical and non-physical components, which is characterised by computing technology and the electromagnetic spectrum for the purpose of modifying, storing, or exchanging data using computer networks. Some researchers define “cyberspace” as a specific environment consisting of a set of computer networks (Kamchatyi, 2017, 153).

Law No. 2163-VIII provides definitions for key concepts related to cyberspace, including “cyberspace”, “cybersecurity”, and “cyber defence”. According to Article 1 of the Law, cyberspace refers to a virtual space that facilitates communication and social

interaction. This space is created through the operation of compatible communication systems that use the Internet or other global data transmission networks.

Clause 5, Article 1 of the Law defines cybersecurity as the protection of important social and state interests during the use of cyberspace. Its purpose is to ensure the development of the information and communication environment, and the timely detection and neutralisation of potential threats to Ukraine's national security in cyberspace.

As per Clause 7, Article 1 of Law No. 2163-VIII, cyber defence refers to a collection of organizational, legal, engineering, and technical measures designed to prevent cyber incidents, promptly detect and protect against all forms of cyberattacks, mitigate the consequences, and restore information, communication, and technological systems.

Given the issues outlined, it is worth noting that the terms “information space security” and “cybersecurity” are relatively new concepts that have arisen from the development of IT technology, as well as input from specialists, consultants, policymakers, and other key stakeholders. The Oxford English Dictionary defines “cybersecurity” as protection against unauthorized use of electronic data or measures adopted to achieve such protection (Voronenko & Tuzhyk, 2017).

The World Economic Forum's Global Risks Report for 2019 identifies cyberattacks as one of the top ten global risks. Between 2017 and 2019, 90% of national critical infrastructure institutions, such as those in the energy, healthcare, industry, and transportation sectors, experienced at least one cyberattack. These attacks had a detrimental impact on their operations, according to the Ponemon Institute (2019).

According to Ye. V. Kotukh, “cyber” is a complex element of the information society that is closely intertwined with various elements of the legal, economic, and political security sectors. Cybersecurity encompasses several important factors, including risk assessment incurred during cyberattacks, emergency recovery, cryptography, and performance of security operations (Kotukh, 2022).

V. F. Antypenko (2013) argues that international partners must take immediate action to protect against and eliminate cyber threats. One of the primary objectives of international law is to support and maintain peace, which cannot be achieved if war is used as a means of national policy. Therefore, international legislation should respond promptly to emerging modern challenges.

The UN General Assembly passed a resolution on December 11, 2000, expressing concerns that the application of science and technology for military purposes could lead to the development of advanced weaponry, including weapons of mass destruction. The UN General Assembly's 1975 Declaration noted with concern that scientific and technological advancements could be used to fuel an arms race or suppress national liberation movements, potentially depriving individuals or peoples of their rights. O. O. Merezhko, a domestic researcher, points out that international law lacks clear criteria for distinguishing simple computer vandalism from attacks that have a serious impact on a state or society (Merezhko, 2010).

According to M. Yu. Yatsyshyn, there are two possible approaches to defining and establishing cyberattacks in modern international law, which shape cyber warfare. This would fall under the purview of international humanitarian law if certain defining criteria are met:

1) Cyber means of influence are classified as military force or military violence.
2) They are carried out within a state or by organized armed groups.

Within the virtual space, borders cannot be clearly defined, making it difficult to determine the origin of a particular cyberattack (Yatsyshyn, 2018).

The initial advancements in the field of informatization and telecommunications date back to 1998, with the research conducted by the First Committee of the UN General Assembly. The primary objective of this committee was to guarantee information security through international collaboration and to engage as many states, private sectors, and civil societies as possible in discussing and addressing pressing issues in the realm of information and digital security. Since 1998, the cyber information space has rapidly developed.

In the event of cybersecurity breaches, the task of bodies combating cybercrime is to determine which specific international laws need to be invoked to address violations in cyberspace. Cybersecurity is recognized as a transnational task at the international level, aimed at protecting against unauthorized influences. This is a common goal of all civilized countries. Efforts to overcome cyber threats demonstrate an increase in international security in the cybersphere. However, they also highlight the need to find new ways, measures, and guarantees that can effectively combat and neutralise cyber threats.

It is worth noting that international law is based on national cybersecurity strategies of individual states and regional security strategies when it comes to cyber defence and the realisation of global public interests in the event of a global threat. Thus, at the regional level, cybersecurity is implemented according to a number of principles, including:

- administrative-territorial organisation of cyber defence of society, protection of places and objects of critical infrastructure that may be subject to cyberattacks;
- an integrated comprehensive approach to the organisation of cybersecurity in a particular region;
- inseparability of security from the development of society and the state, etc.

Cybersecurity cannot be effectively ensured at the regional level. However, effective mechanisms should be put in place to facilitate protection within small territorial units, as well as at the national and international levels (Danyk, 2019, 57-58).

According to K. Spansion, cyberattacks are weapons of terrorist states during hybrid wars. Following the full-scale invasion, cyberattacks have become a frequent occurrence in various sectors of the domestic economy and society, including the government and economy. It is important to note that humanity's reliance on cybersecurity has created significant challenges, not limited to a single country. The energy, medical, economic, and state sectors have been the primary targets of cyberattacks recently.

When discussing economic stability, it is important to note that interference in the state's financial sector has a negative impact on all of its activities (Spansion, 2022).

According to researcher S. B. Tsybenko, a state should aim to end any digital conflict or intervention. Any security measures taken to protect against cyber threats must adhere to the international standards outlined in the 1950 Convention (Tsybenko, 2022).

The international community is actively responding to issues related to the protection of privacy, personal data, and information security as the protection of human rights, freedoms, and privacy rights is recognised as a worldwide priority. However, cybercrimes are now recognised as a serious threat to international peace and security. Several states have committed to combating cybercrime and cyberterrorism through close and productive international cooperation in the fields of law and security. This cooperation involves monitoring technologies, communications, and resources used as tools for committing crimes on the Internet. Significant progress has been made

recently in developing norms of bilateral and multilateral cooperation to combat cybercrime (Cybersecurity, 2021).

The opinion of S. Fedoniuk regarding the increasing complexity of information security issues with each passing year is noteworthy. This is primarily due to the development and application of information and communication technologies and network interactions. However, this exacerbation does not exclude world politics. Currently, there is competition among influential political actors, namely the most powerful states in the world, and their external and internal strategies in the development of information security.

From a policy perspective, there are generally two different views on information security. Some states implement norms that entail strong government control over information, while others support a position that may threaten political stability. The world has divided into centres where their own concepts and visions regarding the protection of the information space from cyberattacks and threats have been developed (Fedoniuk, 2022).

The Prosecutor of the International Criminal Court, K. Khan, has stated that cyber-crimes may fall under the jurisdiction of the ICC if they meet the requirements of the Rome Statute (1988). Cyberattacks, according to the prosecutor, can have the same impact as armed attacks, but without the physical presence of a perpetrator. They can result in human rights violations, destruction of critical infrastructure, loss of property, and other valuable resources. Therefore, it is necessary to review the institution of international law to ensure that all instruments interact comprehensively and effectively.

As such, the prosecutor proposes expanding the application of the Rome Statute of the ICC to cyberspace. International criminal law, by its nature, refers to cases that occurred in the past. However, it is crucial to look ahead and focus all efforts on finding new ways to combat cybercrime (Khan, 2024).

According to Ukrainian cyberspace researcher I. V. Diorditsa, to prevent cyber threats and their negative consequences, it is important to create a legitimization plan. This involves developing and enshrining legal definitions at the legislative level to avoid misunderstandings and discrepancies in their application by different states. These procedures can help prevent collisions with other regulatory acts, define their content, and establish legal practices (Diorditsa, 2017, 100).

5 Discussion

Leading European countries are compelled to take decisive action to combat cyberattacks. Since the 1990s, EU countries have been actively developing and implementing measures to enhance protection against cyberattacks. There have been discussions in the international legal space for a long time regarding the regulation of cyberspace. However, discussions were brought to an end and a shift towards direct action was made due to constant interference in the cybersecurity of countries.

It is important to note that countries are often interdependent in both informational and conceptual aspects when studying cybersecurity threats. This becomes evident when one state depends on another. Ukraine was such a state until recently. Furthermore, Europe has not consistently been willing to counteract Russia's information aggression and establish an effective policy to combat disinformation (Diorditsa, 2015).

In today's society, every state faces the urgent challenge of ensuring information security in the face of cyber threats. The yearly global cybersecurity evaluation raises significant concerns regarding the inadequate protection of citizens in the current information landscape. The spectrum of problems varies widely, from technical weaknesses of a state to vulnerabilities in its systems (Maria Claudia Menezes Leal Nunes, 2021).

It is advisable to establish partnerships between leading countries to quickly respond to unlawful incidents caused by cyberattacks. To effectively combat cyberattacks and unauthorized breaches, it is important to strengthen not only the legal sphere of protection but also the economic, political, social, and security sectors. It is crucial to address the human factor as well, as many employees lack the knowledge to properly respond to external threats. Only IT professionals can recognize subtle cyberattacks. Standard rules should be developed for employees to follow in case of a suspicious situation.

The development of a national cybersecurity system capable of adequately protecting the country's information space is currently the most important task for many international organizations. The state of cybersecurity in Ukraine over the past two years of full-scale intrusion has shown not such a weakness after all. Various cyberattacks from aggressors have demonstrated that the domestic cyber system is capable of resisting external threats. According to the international agreements it has concluded, Ukraine cooperates in the field of cybersecurity with leading countries worldwide, including their defence departments. At the same time, Ukraine directs its efforts towards consolidation and close cooperation with NATO countries in joining the collective cybersecurity assurance system.

Currently, Ukraine is actively leveraging the experience of NATO and other state agencies of member countries to develop a national cybersecurity system. Organising resistance to cyber threats, implementing information and communication security standards, and developing technical capabilities of Computer Emergency Response Teams (CERT) to respond to cyber incidents are all included in cybersecurity. Due to hybrid warfare and e-governance, cybersecurity is a top priority for Ukrainian state policy.

Therefore, like the rest of the world, the level of protection against cyberattacks in Ukraine is inadequate. Although international cooperation in this area continues, no country can claim to be completely protected from all cyber threats. However, achieving the goals of the state and society requires collective efforts to combat cybercrime. Reforms that have already been implemented are yielding positive results (Dumchykov, 2022). Collaboration with international partners, public, governmental, and non-governmental associations to protect against cyber threats is yielding positive results.

Regarding the contribution of non-governmental organizations and society in combating cybercrime, it is important to note that their primary role is to prevent criminal violations in cyberspace by ensuring greater internet network security. One of society's main responsibilities is to use licensed equipment, protective software, exercise caution when using PCs and internet resources, and protect personal data. Considering these measures can improve overall internet security and reduce the number of cybercrimes (Holub, 2016).

Modern cyberattacks often have a latent period lasting several months, making timely detection difficult. Therefore, experts must regularly search for new forms of protection. Effective cybersecurity requires comprehensive and constant application of innovative developments and cutting-edge technologies. To ensure a high level of protection, continuous research and development in cryptography, steganography, and technical security are necessary. A comprehensive approach is required to achieve the desired result and create a reliable network that is no longer vulnerable to external threats.

Considering the new information security strategies of leading countries, international bodies have prioritised addressing cybercriminals' use of the internet to carry out cyberattacks. To achieve this, these institutions are actively developing and implementing effective strategies and mechanisms to prevent the dissemination of harmful materials on the internet.

6 Conclusions

The level of effective functioning of Ukraine's domestic cyber system can be indicated by the country's international cooperation and the experience of leading countries in the field of cybersecurity. In today's world, threats are constantly evolving, and criminals are increasingly using new resources to weaken national security, seize personal data, or obtain other valuable information. After researching the issue, it is important to note that the security of the world is increasingly threatened by cybercrime each year. The main focus in countering cybercrime is currently on improving international legal norms and balancing legislation among leading countries worldwide. The continuous advancement of scientific and technological progress leads to new forms of cyberattacks. However, most of these attacks do not cause significant harm, and their consequences can be restored relatively quickly in most cases.

Literature:

1. Antipenko, V. F.: Regarding the problems of the effectiveness of international law. *Bulletin of Kharkiv National University named after N. V. Karazina*, 2013, 58-60.
2. COVID-19 Makes Universal Digital Access and Cooperation Essential: UN Tech Agency, 2020. https://news.un.org/en/story/2020/05/1063272
3. Cyber security: Council adopts conclusions on EU cyber security strategy: European Council, Council of the European Union, 22 March, 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-theeu-s-cybersecurity-strategy/
4. Cybercrimes may fall under the jurisdiction of the ICC - Prosecutor Khan, 2024. https://www.ukrinform.ua/rubric-world/3816924-kiberzlocini-mozut-pidpadati-pid-urisdikciu-mks-prokuror-han.html
5. Danyk, Y.G.: Fundamentals of CyberSecurity and Cyber Defense. *Odessa: ONAZ named after O.S. Popova*, 2019, 320 p.
6. Diorditsa, I.: The concept and content of cyber threats at the modern stage. *Entrepreneurship, economy and law*, 2017, 4. http://pgp-journal.kiev.ua/archive/2017/4/22.pdf
7. Diorditsa, I.V.: Information interventions as a threat to cyber security. *Legal Sciences*, 2015. http://surl.li/rpdoi
8. Dumchikov, M. O.: Comparative analysis of criminal law protection of cyberspace in the Baltic countries and Ukraine. *Crime prevention: problems of practice and scientific and methodological support*, 2022, 73-80. http://www.sulj.oduvs.od.ua/archive/2022/4/part_1/12.pdf
9. Fedonyuk, S.: Concepts of information security in the aspect of the interests of the main international actors. *International relations, public communications and regional studies*, 2022. https://www.relint.vnu.edu.ua/index.php/relint/article/download/237/257
10. Golub, A.: Cybercrime in all its manifestations: types, consequences and methods of combat. *A safe city*, 2016. http://safe-city.com.ua/kiberzlochynnist-u-vsihyiyi-proyavah-vydy-naslidky-ta-sposoby-borotby/
11. Kamchatnyi, M. V.: Principles of limiting the conduct of cyber warfare in the international information space. *Series: Law*, 2017, 45(2), 152-158.
12. Kotukh, E.V.: Theoretical and methodological foundations of ensuring cyber security in the public sector. *Kharkiv: National University of Civil Defense of Ukraine*, 2022, 479 p. https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disKotukh.pdf
13. Merezhko, O.O.: Problems of the theory of international public and private law. *Kyiv: Justinian*, 2010, 320 p.
14. Nigreeva, O. O.: Regarding the issue of the international legal regime of cyberspace. *Proceedings of the International Scientific and Practical Conference "IT Law: Problems and Prospects for Development in Ukraine (Fourth International Annual Conference)"*, 2020. http://dspace.onu.edu.ua:8080/bitstream/123456789/31497/1/1-7.pdf
15. Novytskyi, V. Ya.: Issues of legal regulation of information and cyber security in modern world politics: international legal aspect, 2021, 84-91. https://ep.unesco-socio.in.ua/wp-content/uploads/2021/05/84-_Novytskyj.pdf
16. Nunes, M. C.: Cyberspace: problems of norm-making. *Revista Conjuntura Global*, 2021, 10, 1, 178–194. https://doi.org/10.5380/cg.v10i1.78424
17. On electronic telecommunications: Law of Ukraine. No. 1089-IX dated December 16, 2020. https://zakon.rada.gov.ua/laws/show/1089-20#n2246
18. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine No. 2163-VIII dated October 5, 2017. https://zakon.rada.gov.ua/laws/show/2163-19#Text
19. On the use of scientific and technological progress in the interests of the world and for the benefit of humanity: Declaration of the UN General Assembly of December 9, 1975. http://surl.li/rpdql
20. Ponemon Institute LLC.: Cybersecurity in Operations Technology: 7 Ideas You Need to Know. March, 2019. https://lookbook.tenable.com/ee2b2c72-e552-43f6-843e-3a63a29d895c
21. Rome Statute of the International Criminal Court. 1998. https://zakon.rada.gov.ua/laws/show/995_588#Text
22. Spansion, K.: Protected in Digital: What International Law Means for Cyberspace Protection, 2022. https://mind.ua/openmind/20244810-zahishcheni-v-cifri-shcho-peredbachae-mizhnarodne-pravo-v-zahisti-kiberprostoru
23. Tsybenko, S. B.: International and European guarantees of ensuring human rights in cyberspace. *Legal scientific electronic journal*, 2022, 5. http://lsej.org.ua/5_2022/161.pdf
24. Voronenko, I. V., Tuzhik, K. L.: Conceptual principles regarding the regulation of cyberspace. International aspect. *Economy. Management. Business*, 2017, 4(22). https://Johnals.dut.edu.ua/index.php/emb/article/view/1664/1590
25. Yatsyshyn, M. Yu.:. Use of force in cyberspace within the framework of international law. *Information and law*, 2018, 4(27). https://ippi.org.ua/sites/default/files/5_11.pdf

Primary Paper Section: A

Secondary Paper Section: AG