ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың «ǴYLYM JÁNE BILIM - 2024» XIX Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIX Международной научной конференции студентов и молодых ученых «ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS of the XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

УДК 341.1/8

THE NEXUS BETWEEN THE CYBERLAW AND INTERNATIONAL ENVIRONMENTAL LAW

Nurgaziyeva Diana Azizbekkyzy
dinanurgazieva4@gmail.com
1st year student of the 7M04202 "International Law", L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Scientific adviser – R.D. Akshalova

As societies digitize their environmental monitoring and management processes, they become vulnerable to cyber threats. Exploring the connection between cyberlaw and international environmental law helps identify potential risks to environmental data integrity and systems, crucial for effective environmental policymaking.

The aim of this article is to investigate the intricate relationship between legal frameworks governing cyberspace and those governing international environmental matters.

Objectives of the article:

- to consider the definition of "cyberlaw,"
- to review cyber threats and their potential impact on environmental security
- to consider the gaps in legislation and the need for its improvement

The objects of the work are the legal frameworks governing cyberspace and international environmental matters.

The subjects of work are the intersection, implications, challenges, and opportunities arising from the interaction between cyberlaw and international environmental law.

Definition of cyberlaw

John O. Adeika defines "cyberlaw" as "the law that regulates activities in cyberspace" [1]. Although there is still no unified understanding of cyber law to this day, some definitions indirectly point to its nature. For example, UNCITRAL defines cyberlaw as "the law governing electronic transactions, particularly those conducted via the internet. It covers contracts entered into electronically, the protection of privacy and personal data, and electronic intellectual property issues". [2] The ITU defines cyberlaw as "the legal framework that regulates cyberspace, encompassing laws related to telecommunications, electronic commerce, data protection, cybersecurity, and digital rights" [3]. The IGF defines cyberlaw as "the body of law governing interactions on the internet, including issues such as online privacy, data protection, cybersecurity, digital rights, electronic commerce, and intellectual property" [4].

In the cyber security standard ISO/IEC 27032:2012 "Information technology - Security techniques - Guidelines for cybersecurity," "cyberspace" is defined as "the complex environment resulting from the interaction of people, software, and services on the Internet using technology, devices, and networks connected to it, which do not exist in any physical form" [5].

The international legal framework in the field of cybersecurity consists of universal, regional, and national regulatory acts in this area. For example, in Resolution A/70/237 (2015), the UN Charter is proclaimed to apply, including to cyberspace, officially recognizing cyberspace as significant as physical space. Resolution A/73/27 (2018) established states' responsibility in the use of ICT for malicious purposes. Resolution A/76/439 (2021) largely reiterated the provisions of previous resolutions without introducing any new provisions [6]. UN regulatory acts in the considered area comprise over 30 documents. However, as noted by professors Zakharova A.I. and Sidorov T.Y., they have the character of "soft law" since they do not establish specific norms in the field of international information law [7].

For instance, the EU Cybersecurity Act of 2019 granted the European Union Agency for Network and Information Security the mandate to collect and monitor necessary information and analytical data from companies and institutions to effectively respond to and prevent cyber incidents [8]. Similarly, national legislation such as Kazakhstan's Cybersecurity Concept for the period 2017-2022 has its regulatory acts regulating the considered area, indicating the emerging nature of cyber law [9].

In general, the documents and interpretations of cyber law discussed above allow us to draw the following conclusion: the object of regulation of cyber law is cyberspace, which is subject to various cyber threats.

Cyber threats and their potential impact on environmental security

Many environmental systems, including water treatment facilities, power plants, and environmental monitoring networks, heavily rely on information technology and networked systems. These critical infrastructures face vulnerability to cyber attacks, risking operational disruptions and potential environmental disasters. Professor W.H. Boothby, co-author of NATO's Tallinn Manual, highlights the potential of cyber weaponry to cause severe environmental damage, such as a nuclear meltdown or compromise of vital oil pipelines like the Colonial Pipeline. The Stuxnet worm incident exemplifies the risk, as it targeted Iran's nuclear program, damaging uranium enrichment centrifuges [10]. Similarly, cyber attacks on the oil industry, like the 1999 Gazprom attack and the 2016 Kemuri water company attack, underscore the tangible threats posed. A survey of energy, oil, gas, and utility industry professionals reveals widespread concern, with 94% having experienced cyber-criminal targeting, and 83% acknowledging the potential for serious physical harm from cyber attacks [11].

Jan Kallberg notes that Three Mile accident illustrates the potential consequences of disruptions to critical systems. In terms of cyber threats, the connection to the Three Mile Island accident lies in the broader context of critical infrastructure vulnerabilities. The Three Mile Island accident, which occurred in 1979 in Pennsylvania, was a pivotal event in the history of nuclear energy in the United States. A combination of technical malfunctions and human errors led to a partial meltdown of one of the reactors at the Three Mile Island Nuclear Generating Station. While the accident resulted in limited radioactive release and no immediate fatalities, it significantly damaged public confidence in nuclear power and had far-reaching consequences for the nuclear industry [12]. Thereby he claims that it is crucial for cyber resilience to look beyond the information systems.

Considering the potential of cyberweapons, Guardio Research Team claims that "in the most extreme cases, cyberattacks could even lead to loss of life. For example, if an attacker gained control of a water treatment plant, they could contaminate the water supply with harmful chemicals. Or, if they took over a power grid, they could cause widespread blackouts" [13].

Continuing the topic of critical infrastructure vulnerability to cyber attacks, it is worth noting that cybersecurity has been a sore spot for water systems for many years. Similar to other critical infrastructure, the sector is fragmented and underfunded, so it's less able to keep up with evolving threats. Two hacks on water systems by cyber gangs show the ongoing vulnerability of critical infrastructure (The Municipal Water Authority of Aliquippa in Pennsylvania was attacked) [13].

Environmental Risk Consulting Team has published an environmental white paper, where they have listed the cyber attacks and cyber crimes which have shown the vulnerability of critically crucial infrastructures [14]:

2014 - A cyber attack against a German steel mill's industrial control system caused substantial damage to the blast furnace [14].

2015 - A cyber attack against the power grid in Ukraine switched off 30 substations, leaving 230,000 people without power for up to six hours. The attack included seizing SCADA systems, disabling/destroying IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators), destroying hardware, and launching denial of service attacks on call centers [14].

2017 - A cyber attack against a Saudi Arabian petrochemical plant, where the intention was to sabotage the firm's operations and trigger an explosion. Investigators said the only thing that prevented an explosion was an error in attacker's computer code that inadvertently shut down the plant’s production systems. Proof of concept cyber attack against dozens of US power companies, where data and critical systems were compromised to the point where they could have been sabotaged and had power shut down. Hacked systems details included company operations, engineering plans and equipment, and possible control of valves, pipes or conveyer belts. It is believed the purpose of the attack was to prove that whatever government or organization was behind the attacks was capable of having such potential impacts. It is the initial attacks that were launched using email phishing campaigns [14].

2018 - A combined phishing and ransomware attack on the City of Atlanta occurred and was quickly recognized. The attack stopped people from accessing applications to pay bills and access court related documents. The city had to shut down many digital services such as its court system database and the Atlanta International Airport Wi-Fi [14].

2019 - Employees at over 200 oil & gas machinery companies around the globe were targeted with attempts to steal corporate secrets and erase data from computers [14].

Gaps in legislation and the need for its improvement

From the examples above, we have seen that cyber threats have the potential to cause real damage to environmental security. In connection with this, as many researchers have emphasized, strengthening the cybersecurity of critical infrastructure is important. Below, we will consider the international mechanisms available in this area.

"Critical Information Infrastructure" (CII) refers to state institutions and other important facilities whose compromise could have a negative impact on personal, societal, or state security [15]. The first session of the United Nations Government Expert Group on Information Space Codification was held in 2004, with experts from countries such as Belarus, Brazil, Germany, India, Jordan, China, Malaysia, Mali, Mexico, South Korea, Russian Federation, United Kingdom, United States, France, and South Africa participating. Following the conclusion of the session, which consisted of three meetings, the UN General Assembly published the Report of the Government Expert Group (2005) [6]. The report highlighted the high vulnerability of CII at both the national and international levels and underscored the danger posed by the use of ICT by non-state actors (individuals, multinational corporations, organized groups, terrorists, etc.). Additionally, it addressed the issue of states enhancing ICT capabilities for military purposes.

In its resolution "Achievements in the field of Informatization and Telecommunication" of December 5, 2018, the General Assembly once again emphasized that states should not take measures that could endanger the CII of another state or the international community. It also stressed that states are solely responsible for ensuring the security of their citizens and CII; however, some states, due to low technological development, may not be able to provide adequate protection, thus the international community should assist such states [6].

The most significant contribution has been made by the legislative acts of the European Union, which introduced a new type of cybersecurity policy - "cyber resilience". The Network and Information Systems Security Directive 2016, Network and Information Systems Security Directive 2020, and Cyber Resilience Act 2022 aim to establish regulatory frameworks to ensure cyber resilience [16]. Cyber resilience is the ability to quickly return to a stable state after encountering problems. Therefore, EU's cyber resilience policy is built in collaboration with the private sector. As noted by expert Kovalev O.G., cybercrime in EU documents is closely linked to information structure. One form of combating cybercrime is "intercepting criminal activity related to cyberattacks on information systems, including situations where crime is provided as a service" [16]. The 2016 directive established the responsibility of member states for technical and regulatory response to cyberattacks, including in sectors such as energy, transportation, water supply system, banking system, finance, healthcare, etc. [17]. According to this document, all companies operating in these sectors were required to report cyber incidents to the government.

Despite the global trend towards strengthening the cybersecurity of critical infrastructure, international legal norms in this area still have a soft character. Although many states are implementing legislative acts emphasizing the importance of cybersecurity policy (for example, the "Cyber Protection" Concept of Kazakhstan highlights the need to strengthen information infrastructures [9], and the 2020 U.S. National Security Strategy identifies cybersecurity policy as one of the priority areas of development [18], etc.), there are still many unresolved issues. For instance, the "Cyber Protection" Concept indicates that "computer attacks launched from foreign territory should be maximally prevented at the 'electronic border' - the virtual perimeter of the country” [9]. However, as experts from the Stevens Institute of Technology note, tracing sources of cyber attacks remains challenging. Furthermore, the introduction of the concept of "digital sovereignty" gives states the opportunity to exercise the right to self-defense, according to Article 51 (UN Charter [19]).

Conclusion

In conclusion, cyberlaw is an emerging area of law that regulates cyberspace. One of the main objectives of cyberlaw is to ensure cybersecurity in cyberspace by addressing cyber threats.

The processes of digitization and globalization have also affected the sphere of environmental protection. Thus, we have witnessed that one of the trends in recent years, especially in the implementation of sustainable development policies, is the digitization of various sectors, making the formation of information infrastructure one of the priority areas of activity for countries in recent years. The term "information infrastructure" or "critical information infrastructure" refers to state institutions and other important facilities whose compromise could have a negative impact on personal, societal, or state security. According to a report by a group of UN government experts dealing with the codification of cyberspace, information infrastructure is one of the vulnerable elements of cyberspace because it is subject to frequent cyber attacks.

In general, analyzing the challenges and threats to environmental security from cyber technologies, the following can be highlighted:

1) Threats to critical infrastructure,

2) Threats associated with the failure of electronic systems of objects that are of importance and have the potential to cause environmental damage (such as nuclear power plants, oil pipelines, etc.),

3) Threats associated with sustainable development goals (disruption of water supply systems, power supply - "A cyber attack against the power grid in Ukraine switched off 30 substations, leaving 230,000 people without power for up to six hours," and so on) impede the achievement of sustainable development goals.

Thus, we have identified that risks to environmental security are primarily related to ensuring the cybersecurity of critical information infrastructures. Analysis of international legal practice in this area has helped identify that the response to these threats and challenges could be the implementation of cyber resilience policies, actively applied within the framework of the European Union. However, besides this, there are still many unresolved issues, such as the question of accountability for internationally unlawful acts in cyberspace and the absence of a universally recognized procedure for identifying the perpetrator, issues concerning the boundaries of "digital sovereignty," and the associated issue of the applicability of the right to self-defense, according to Article 51 of the UN Charter, in cyberspace.

In our view, the first step in addressing these issues should be the adoption of an international document regulating cyberspace and possessing legally binding force.

References

1. John O. Adeika Cyberlaw – Standars and Legal Issues [Electronic source].-URL: https://www.researchgate.net/publication/280882159_Cyberlaw__Standard_and_Legal_Issues. – Date of access: 02.03.2024.
2. UNCITRAL Model law of Electronic commerce 1996 [Electronic source].-URL: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce– Date of access: 02.03.2024.
3. ITU Understanding cybercrime: phenomena, challenges and legal responses [Electronic source].-URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeE.pdf - Date of access: 02.03.2024.

4. IGF 2019 [Electronic source].-URL: https://www.intgovforum.org/en/content/igf-2019-ws-165-round-table-on-cyberlaw-cybercrime-cybersecurity - Date of access: 02.03.2024.

5. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века // Вопросы кибербезопасности, №1, 2013, С.2-9.

6. Крутских А.В. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке). – М.: «Аспект Пресс», 2019, 784с.

7. Сидоров Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН // Сибирский юридический вестник, №3 (90), 2020, С. 103-108.

8. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности, №3 (11), 2015, С.2-1.

9. Об утверждении концепции кибербезопасности («Киберщит Казахстан») [Электронный ресурс].- Режим доступа: https://adilet.zan.kz/rus/docs/P1700000407 . - Дата обращения: 02.03.2024.

10. William H. Boothby Methods and Means of Cyber Warfare [Electronic resource].- URL: https://www.hsdl.org/c/view?docid=734393 – Date of access: 09.03.2024.

11. George Stergiopoulos Cyber-Attacks on the Oil&Gas Sector: A survey on Incident Assessment and Attack Patterns [Electronic resource].- URL: https://www.researchgate.net/publication/342790008_Cyber-Attacks_on_the_Oil_Gas_Sector_A_Survey_on_Incident_Assessment_and_Attack_Patterns – Date of access: 08.03.2024.

12. Jan Kallberg Cyberattacks with environmental impact- high impact on societal sentiment [Electronic resource].- URL: https://cyberdefense.com/2018/10/30/cyber-attacks-with-environmental-impact-high-impact-on-societal-sentiment/ – Date of access: 06.03.2024.

13. Guardio research team Why environmental services and infrastructure are vulnerable to cyberattacks [Electronic resource].- URL: https://guard.io/blog/why-environmental-services-and-infrastructure-are-vulnerable-to-cyberattacks – Date of access: 02.03.2024.

14. Environmental risks: cyber security and critical industries [Electronic resource].- URL: https://axaxl.com//media/axaxl/files/pdfs/insurance/cyberenvironmentalrisks_whitepaper_us_ca_axa-xl.pdf– Date of access: 06.03.2024.

15. Каратаева Л.Р. Информационная безопасность vs кибербезопасность: проблемы определения // Казахстан-Спектр. – №1. - 2014. – С. 5-13.

16. Ковалев О.Г. Нормативно-правовое регулирование реализации стратегии кибербезопасности в государствах Европейского Союза // Столыпинский вестник, №2, 2021, С. 30-42.

17. The Network and Information Systems Security Directive 2016 [Electronic resource].- URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj – Date of access: 06.03.2024.

18. 2020 U.S. National Security Strategy [Electronic resource].- URL: https://nssarchive.us/ – Date of access: 06.03.2024.

19. UN Charter [Electronic resource].- URL: https://www.un.org/en/about-us/un-charter Date of access: 06.03.2024.