GIS Odyssey Journal

2023 • Volume 3 • Number 1

https://doi.org/10.57599/gisoj.2023.3.1.31

Kamil Strzępek[1]

DEFINED CYBERSECURITY THREATS IN UNDEFINED CYBERSPACE

Abstract: In the literature on the subject and international legal acts, there is no universal and common definition of cyberspace. Due to the above lack, countries are moving towards regional cooperation in cybersecurity. This descriptive-analytical research was conducted to illustrate cybersecurity threats (faced by countries and private individuals), the list of which, as a result of digital transformation, is constantly growing. The analysis results presented that a wide range of potential cyber-attacks may affect objects of a tangible and intangible character. This research suggests that in cyberspace, which is essentially intangible, non-physical targets (values) can also be an object of a cyber-attack.

Keywords: cyberspace, cybersecurity threats, cyber-attack, critical infrastructure

Received: 28 June 2023; accepted: 03 August 2023

[1] Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration, Poland, ORCID ID: https://orcid.org/0000-0001-9277-6057, email: k.strzepek@uksw.edu.pl

Introduction with analysis of the state of the problems

It seems that nowadays, the prevailing view is that international law does not prohibit the state from regulating its "segment" of cyberinfrastructure, although this right should be implemented taking into account the principles of international law (Ivanova et al., 2022). Cyberspace is expanding in many directions without a clear teleology. This does not prevent us from theorising about the nature of cyberspace, but we should refrain from overly ambitious or deterministic claims (Lambach, 2019). At the same time, it still seems valid that cyberspace is not an apolitical sphere of non-state actors. On the contrary, it is a domain in which countries seek to exercise their sovereignty. As a result, managing cyberspace resembles a power politics game (Liaropoulos, 2017).

However, in the absence of an international, universal consensus regarding the legal status of cyberspace, countries are moving towards regional cooperation, primarily regarding the so-called cybersecurity, which is currently the main regulatory area of cyberspace (Wielec et al., 2023).

The purpose of this paper is to present key issues related to the issue of cybersecurity and the main threats to this security. The following questions were discussed (structure of the paper): 1) cybersecurity strategies of selected countries and their goals; 2) operational activities in cyberspace and cyber-attack; 3) cybersecurity threats; 4) the issue of critical infrastructure; 5) conclusions.

Material and Methods

This research was conducted in 2023. The research was based on legal acts of states and international organisations as well as on scientific and popular science literature. The research method used in the paper was a descriptive analysis (Portman, 1986) and interpretation of recent trends in the area of cybersecurity threats and operational activities in cyberspace. Based on the conducted research, it was possible to identify potential objects of a cyber-attack that may also be of an intangible character, i.e., values that create our "common good".

Cybersecurity

The concept of cyberspace is inextricably linked to the concept of cybersecurity, which at the most basic level can be understood as: 1) confidentiality - ensuring that unauthorised persons will not obtain information; 2) integrity - ensuring that information will not change its form in an unauthorised manner, for example, there will be no unwanted modifications; 3) availability – ensuring that the ability to use systems, data, information and resources will not be lost (Olejnik et al., 2022).

The definition mentioned above corresponds to the definition developed by the International Telecommunication Union, which reads as follows: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and a user's assets.

Organisation and a user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, and Confidentiality" (International Telecommunication Union, 2023).

Countries refer to international cooperation in the field of cybersecurity (or more generally in the field of activities in cyberspace) in their National Cybersecurity Strategies (NCSS). Some countries only mention "international cooperation" in general terms. Some countries are a bit more precise and refer to "regional" or "multilateral" cooperation or cooperation within a "specific international organisation" or "bloc of states". Some countries refer to cooperation with "strategic partners" or "like-minded countries" (Serrano Iova et al., 2023). The most mentioned "country bloc" was the European Union-EU, with appearances in twenty-six individual NCSS, and the most mentioned organisations were the North Atlantic Treaty Organization-NATO, the United Nations-UN and the Organization for Security and Co-operation in Europe-OSCE, with eighteen, sixteen and thirteen mentions respectively (out of 194 countries analysed) (Serrano Iova et al., 2023).

The EU adopted (being still in force) Directive (EU) 2016/1148 of the European Parliament and the Council on 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. This directive, among other things, made it mandatory for all EU Member States to adopt a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented, set up a cooperation group to support and facilitate strategic cooperation and information exchange between EU Member States and to develop trust and confidence among them; established a network of computer security incident response teams (the so-called CSIRT's Network); established obligations for Member States to designate national competent authorities, points of single contact and CSIRT with tasks related to the security of network and information systems.

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 distinguishes the main objective, which is to increase the level of resistance to cyber threats and increase the level of information protection in the public, military and private sectors, and to promote knowledge and good practices enabling citizens to protect their information better, as well as specific objectives, such as 1) development of the national cybersecurity system; 2) increasing the level of resilience of the administration's information systems; 3) increasing the national security potential; 4) building awareness and social competence in the field of cybersecurity; 5) building a strong international position of the Republic of Poland in the area of cybersecurity (Resolution no. 2 of the Council of Ministers of the Republic of Poland, 2019).

Odebade and Benkhelifa compared the NCSS contained in publicly available documents of ten countries in Europe (UK, France, Lithuania, Estonia, Spain and Norway), Asia-Pacific (Singapore and Australia) and the US region (United States of America and Canada) and came to the conclusion that common goals of the NCSS regarding network and information systems security strategy can be considered building a cybersecurity culture through education, fostering international cooperation, promoting research and development, promoting cyber awareness and creating an environment of trust in cyberspace where citizens, businesses and government can operate (Odebade et al., 2023).

At the same time, these authors indicated some unique goals in relation to the NCSS of the discussed countries. It is worth paying attention to the objectives contained in the Norwegian cybersecurity strategy, which mentions, among other things, that Norwegian companies will digitalise in a secure and trustworthy manner and be able to protect themselves against cyber incidents (Odebade et al., 2023). This is interesting because the document sets a goal for Norwegian companies, i.e., private entities, to be able to protect themselves against cyber incidents. In a government document, this type of task should be assessed positively. Ensuring cyber security for private entities or people cannot rest solely on the state and its authorities. Another interesting issue in this context is when an action in cyberspace aimed at a private company will cause the state and its authorities to react. Should a boundary be drawn, defining when a private company defends itself against cyber incidents and when the state and its authorities intervene? It seems that the answer to such a question should be negative, i.e., there should be no boundary defining when an attack on a private company will be covered by the state's and its authorities' intervention. The defined border, describing the circumstances in which the state and its authorities intervene, could be skilfully used by those launching attacks. Moreover, it could discourage private companies from taking action in the field of their own cybersecurity. Private companies exercise substantial autonomy over "their" territories (Lambach, 2019).

In the context of private companies, it is also worth mentioning that the cyber domain is based primarily on infrastructures created by global private companies (e.g., Microsoft, Cisco, Oracle), which are located in each country and are interconnected.

Also interesting is the goal included in the NCSS of the United States, which is to protect the American people, the homeland and the "American way of life" (Odebade et al., 2023). The latter should be understood as the values that stand behind a civilised nation, in which, among other things, civil rights and freedoms are respected. Undoubtedly, the purpose of protection formulated in this way sheds new light on concepts such as, for example, the concept of "common good". It also indicates that not only tangible goods are subject to protection, but also intangible ones, i.e., values.

Operational activities in cyberspace and the basic features of a cyber-attack

Four operational activities can be distinguished in cyberspace (Chmielewski, 2022):

1. Communications and Information Systems Infrastructure Operations-CISIO;

2. Cyberspace Intelligence, Surveillance and Reconnaissance Operations-CISRO; 3. Defensive Cyber Operations-DCO; 4. Offensive Cyber Operations-OCO.

Some argue that cyber capabilities are "one-time use": when a cyber operation exploits a certain vulnerability, it becomes known to the public and thus loses its usefulness. Knowing this, other potentially attacked can effectively defend themselves against a similar attack by installing appropriate software patches. Some argue that this is not the case and that it takes a long time for the appropriate patches to be installed and the vulnerabilities to be fixed (Smeets, 2022).

A cyber kill chain is the structure of a cyber-attack seen from the attacker's perspective. We can distinguish the following stages: 1) diagnosis; 2) armament; 3) delivery; 4) exploitation; 5) installation; 6) command; 7) implementation of goals (Olejnik et al., 2022). In other words, it is about finding a way in, finding a way back to your command and control server, and achieving exfiltration and cloaking capabilities (Perlroth, 2022).

A cyber-attack can be carried out by the so-called hacktivists, i.e., an informal group associated with some goal (social, political or any other) (Olejnik et al., 2022). Cybercriminals can also carry out a cyber-attack, i.e., usually organised groups focused mainly on profit (but also on behalf of state authorities) (Olejnik et al., 2022). We can also talk about people who work within state structures, the so-called cyber operators (Olejnik et al., 2022).

The basic features of a cyber-attack are 1) its virtual form; 2) no space limitation; the blurring of the traditional distinction between local and international conflict; 3) malware can travel in information resources and operates using network connections and not according to the rules of geography; 4) the "load" of weapons is also "intangible" - this software is the most direct cause of destruction; 5) causing damage requires a remote object – a controller – that can be manipulated, and the use of code using weapons can have consequences for the political and economic world; 6) the use of cybernetic weapons does not have to lead to physical destruction to constitute a serious threat to the state and its society (Chmielewski, 2022).

Results and discussion

If we assume – as above – that cybersecurity, at a basic, general level, can be understood as confidentiality, integrity and availability, then cybersecurity threats, also at a basic, general level, may lead to 1) lack of confidentiality, i.e. access to information by unauthorised persons; 2) lack of integrity, i.e. introducing changes to information in an unauthorised manner; 3) lack of availability, i.e. the inability to use systems, data, information, resources.

When it comes to the basic types of threats, we can therefore distinguish: 1) illegal access to the system (hacking) (Szpor et al., 2022); 2) breach of confidentiality of communication (sniffing); 3) data integrity violation; 4) destroying, damaging, deleting or changing IT data of special importance, e.g. for the defence of the country (computer sabotage); 5) preventing the use of systems, data, information, resources. Obviously,

many of these actions are reflected in the penal codes of the countries they are penalised.

When it comes to the basic methods of operation, we can distinguish: 1) malware – software or firmware designed to perform unauthorised processes that will adversely affect the confidentiality, integrity or availability of the IT system. A virus, worm, Trojan horse, or other code-based unit that infects a host. Spyware and some forms of adware are also examples of malicious code (Computer Security Resource Center, 2023); 2) ransomware – prevents or restricts users from accessing their system via malware. Ransomware expects you to pay a ransom through online payment methods to regain access to your system or data. Online payment methods often include virtual currencies, cryptocurrencies (the Commonwealth of Massachusetts, 2023); 3) Distributed denial of service (DDoS) attacks that render an online service unavailable because it is overwhelmed by excessive traffic from multiple locations and sources (the Commonwealth of Massachusetts, 2023); 4) acting with unsolicited, unwanted messages and emails (spam); 5) activities aimed at obtaining confidential information. Phishing attempts will look for information coming from a trusted person or company (phishing) (the Commonwealth of Massachusetts, 2023); 6) action, using all available techniques (e.g., baiting), consisting in persuading the victim to disclose certain information or perform a certain action for unjustified reasons (social engineering) (European Union Agency for Cybersecurity, 2023).

In addition to the above-mentioned basic methods of operation, it is also worth paying attention to the increasingly sophisticated cyber-attacks, including not only malware and phishing but also machine learning and artificial intelligence and others, which put the data and assets of corporations, governments and individuals at constant risk (Moore, 2023). It is worth remembering that cyber threats are changing rapidly. Attack tactics and methods change and improve every day.

Understanding the nature of the risks and threats facing the entity so that it can better prepare for them is dealt with by cyber intelligence, which can be considered a component of the entity's cybersecurity system. Cyber intelligence is used to identify a cyber threat. Cyber intelligence helps you understand attackers, their motives, actions and capabilities, and how they operate. It is more than data mining: it requires the ability to analyse what is happening in real-time. Cyber intelligence helps organisations make faster, more informed security decisions and shift their behaviour from reactive to proactive to combat attacks (EC-Council, 2023).

It is also worth pointing out that some also distinguish the concept of cyber-hygiene. Cyber hygiene differs from cybersecurity, but it relates to individuals rather than a group of organisations. While cyber-hygiene is the responsibility of an individual, cybersecurity is the responsibility of a group or organisation and applies only to their professional activities (Singh et al., 2020). An example of good cyber-hygiene practice is keeping your device and system software up to date (Singh et al., 2020).

Critical infrastructure

In the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (the Group was convened by the resolution of the General Assembly of the United Nations on 5 December 2018) of 18 March 2021 stated, among other things, that activities contrary to obligations under international law, which deliberately damage critical infrastructure or otherwise impede the use and operation of critical infrastructure providing services to the population, may pose a threat not only to security, but also for the sovereignty of the state, as well as its economic development and livelihoods, and ultimately for the security and well-being of individuals (Report, 2021).

One of the basic obligations of states under international law is to refrain in their international relations from the threat or use of force against any state's territorial integrity or political independence. While cyber-attack techniques can and probably will evolve, shared values – such as peace – should remain the same. Therefore, it is not worth forgetting values when discussing cyberspace and cyber-attacks. Given what has been said, we can distinguish an object of a cyber-attack of a tangible or an intangible character. This distinction can be useful due to the aforementioned evolution of cyber-attack techniques and even the difficulty of identifying their existence. Sometimes only the effects will be visible, which can be tangible or intangible (non-physical) (like the whole of cyberspace).

A classic example of an object of a cyber-attack of a tangible character is critical infrastructure such as the electricity grid, the water supply network, the financial system, nuclear weapons, etc. (Sanger, 2021). Classically and quite broadly, the concept of critical infrastructure can therefore be understood as "(...) sensitive elements of state infrastructure, necessary for the functioning of the state and society (population)" (Olejnik et al., 2022).

An example of an object of a cyber-attack of an intangible character could be "values" such as peace. The electoral system can be considered a critical infrastructure of an intangible character. If the skeleton of democracy is the ability to conduct free and fair elections, then the state's electoral system can be considered an infrastructure of key importance to the state (Sanger, 2021).

Therefore, from the state's point of view, the most undesirable attacks will be those against elements of its critical infrastructure, both of tangible and intangible character. In addition, attacks on civilians (individuals – Internet users) and legal persons can also be distinguished.

Conclusions

Countries' activities in cyberspace may occur within specific types of operational activities in cyberspace. It can be said that currently, the main area of cooperation between countries in cyberspace is cybersecurity. This is due to the fact that there are several threats, the list of which – due to digital transformation – is constantly growing.

Cyber intelligence deals with identifying threats and understanding the motives of attackers and how they operate, which can be considered a component of cybersecurity.

Particularly important is the issue of cooperation between public authorities and private companies in the field of cybersecurity. Should a boundary be drawn, defining when a private company defends itself against cyber incidents and when the state and its authorities intervene? It seems that the answer to such a question should be negative, i.e., such a border should not be set. The defined border, describing the circumstances in which the state and its authorities intervene, could be skilfully used by those launching attacks. Moreover, it could discourage private companies from taking action on their own cybersecurity. Individuals should also comply with the so-called cyber-hygiene.

Due to the development of regulations in the field of cybersecurity, and the desire to protect goods that may become the object of attack, the concept of the common protective good is being extended. Cyber-attacks on tangible and intangible targets make us aware that the protected good can be of a physical or non-physical character. Such attacks on such tangible and intangible assets may affect the interpretation of such concepts as, for example, the concept of state security.

References

Chmielewski M. (2022). Działania w cyberprzestrzeni. Narzędzia, Organizacja, Metody (*Actions in cyberspace. Tools, Organisation, Methods*) https://www.researchgate.net/publication/366275555_Dzialania_w_cyberprzestrzeni_Narzedzia_Organizacja_Metody [access: 28.06.2023].

Computer Security Resource Center. https://csrc.nist.gov/glossary/term/malware [access: 28.06.2023].

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

EC-Council. (2023). What is Threat Intelligence in Cybersecurity? https://www.eccouncil.org/cybersecurity/what-is-cyber-threat-intelligence/ [access: 28.06.2023].

European Union Agency for Cybersecurity. (2023). What is "Social Engineering"? https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering [access: 28.06.2023].

International Telecommunication Union. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [access: 28.06.2023].

Ivanowa K.A., Myltykbaev M.Zh., Shtodina D.D. (2022). The concept of cyberspace in international law. Law Enforcement Review, vol. 6, no. 4, pp. 32–44.

Lambach D. (2019). The Territorialization of Cyberspace. International Studies Review, vol. 22, no. 3, pp. 482–506.

Liaropoulos A. (2017). Cyberspace Governance and State Sovereignty. In: G.C. Bitros, N.C. Kyriazis (ed.), Democracy and an Open-Economy World Order. Springer, New York City, pp. 25–35.

Moore M. (2023). Top Cybersecurity Threats in 2023. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ [access: 28.06.2023].

Odebade A.T., Benkhelifa E. (2023). A Comparative Study of National Cyber Security Strategies of ten nations. https://www.researchgate.net/publication/369540767_A_Comparative_Study_of_National_Cyber_Security_Strategies_of_ten_nations [access: 28.06.2023].

Olejnik Ł., Kurasiński A. (2022). Filozofia Cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny (*Cybersecurity philosophy. How is the world changing. From malware to cyber warfare*). Wydawnictwo Naukowe PWN, Warszawa.

Perlroth N. (2022). This Is How They Tell Me the World Ends: A True Story. Bloomsbury Publishing, New York City.

Portman C.P (1986). Jurisprudence: A Descriptive and Normative Analysis of Law. Michigan Law Review, vol. 84, Issue 4, pp. 1041–1046.

Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security of 18 March 2021, A/75/816.

Resolution No. 125 of the Council of Ministers of the Republic of Poland of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024.

Resolution of the General Assembly of 5 December 2018, A/RES/73/27.

Sanger D.E. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown Publishing Group, New York City.

Serrano Iova R., Watashiba T. (2023). NCSS: A Global Census of National Positions on Conflict, Neutrality and Cooperation. https://www.researchgate.net/publication/371703348_NCSS_A_global_census_of_national_positions_on_conflict_neutrality_and_cooperation [access: 28.06.2023].

Singh D., Mohanty N.P., Swagatika S., Kumar S. (2020). The key Concept for Cyber Security in Cyberspace. Test Engineering and Management, vol. 83, pp. 8145–8152.

Smeets M. (2022). The Role of Military Cyber Exercises: A Case Study of Locked Shields. In: T. Jančárková, G. Visky, I. Winther (ed.), 14th International Conference on Cyber Conflict: Keep Moving. CCDCOE, Tallinn, pp. 9–26.

Szpor G., Gryszczyńska A. (2022). Hacking in the (Cyber)Space. GIS Odyssey Journal, vol. 2, no. 1, pp. 141–152.

The Commonwealth of Massachusetts. https://www.mass.gov/service-details/know-the-types-of-cyber-threats [access: 28.06.2023].

Wielec M., Oręziak B. (2023). Cyberprzestrzeń i cyberprzestępczość: uwagi dotyczące definicji z elementami analizy prawnoporównawczej (*Cyberspace and cybercrime: comments on definition with elements of comparative law analysis*) In: M. Wielec (ed.), Cyberbezpieczeństwo na rzecz zapobiegania przyczynom przestępczości (*Cybersecurity to prevent crime causes*). Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa, pp. 9–34.