DOMINIK BIERECKI, MIROSŁAW KARPIUK,
CLAUDIO MELCHIOR, NICOLA STRIZZOLO

Security in the Era of Cybersecurity Threats

Abstract

Security has always been of paramount importance to both society and the state. In the era of widespread Internet access, we can speak of a new dimension related to the use of cyberspace. New threats are emerging that are not limited to specific countries but can even have an international dimension. Given that information and communication systems are now widely used around the world, cyberthreats that compromise their functioning are also common. New technologies, including artificial intelligence, are, on the one hand, a manifestation of the development of states and societies, but, on the other hand, if used improperly, they can lead to serious consequences, even disrupting the operation of strategic sectors and even necessitating the activation of crisis management mechanisms. When implementing and using information and communication technologies, the associated risks must also be considered. Electronically transmitted and shared information now occurs on a large scale, so it is crucial to avoid being manipulated. The purpose of this paper is to determine the security status of a digital state that utilises cyberspace for its operations. Within this state, society also benefits from new technologies, which are also based on cyberspace. This paper employs a dogmatic-legal approach and also includes a review of the literature. Therefore, qualitative methods related to text content analysis were used.

DOMINIK BIERECKI – associate professor, Pomeranian University in Słupsk,
ORCID – 0000-0001-6993-3974, e-mail: dominik.bierecki@upsl.edu.pl
MIROSŁAW KARPIUK – full professor, University of Warmia and Mazury in Olsztyn,
ORCID – 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl
CLAUDIO MELCHIOR – associate professor, University of Udine,
ORCID – 0000-0002-6124-4717, e-mail: claudio.melchior@uniud.it
NICOLA STRIZZOLO – associate professor, University of Teramo,
ORCID – 0000-0001-6384-9210, e-mail: nstrizzolo@unite.it

HTTPS://DOI.ORG/10.36128/PRIW.VI57.1476

KEYWORDS: cyberspace, cybersecurity, artificial intelligence, critical infrastructure

1 | Introduction

The state and society are exposed to a number of threats, some of which are related to the operation of cyberspace. Many tasks and services require IT systems for implementation, making such activities cheaper, faster, and more accessible to a larger audience. These systems also make activities more convenient for recipients and providers. While cyberspace offers conveniences, it also poses dangers with potentially far-reaching consequences, including those that affect the stability of the state. Given the prevalence of using cyberspace for public and private business, it is necessary to implement appropriate safeguards against cyberthreats. These mechanisms include technical and legal solutions.

Disruptions in cyberspace can negatively affect society and the state, which is responsible for ensuring the quality of services provided, including those fundamental to citizens. Given the need to adequately secure these services, including ensuring their availability, continuity, speed, and accessibility, it is necessary to take appropriate measures.[1] The state is primarily responsible for these measures because it exists to meet the needs of society, including the need for cybersecurity.

Cyberthreats can be technical or non-technical. Technical threats include malware that aims to damage, destroy, take over, or control IT systems. Non-technical threats are all sorts of activities, behaviors, and phenomena among internet users. These threats are often aimed at identity theft and acquiring confidential information and data. This leads to financial and reputational losses for victims.[2]

The digital ecosystem is currently very important, and in recent years it has opened up new possibilities, both in terms of remote management

[1] Mirosław Karpiuk, „Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź*, No. 4 (2022): 167-168.

[2] Kacper Pirch, "Socjotechnika jako cyberzagrożenie," [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski (Gdynia: Wydawnictwo BP, 2021): 193.

of internal processes and interaction with potential customers around the world. However, the ever-increasing amount of data transmitted via digital channels is directly proportional to the effort that hackers put into creating malware.[3] Technological evolution forces us to develop increasingly effective solutions to counteract the misuse of IT tools, which may threaten the security of people or the state.[4]

2 Cybersecurity and its threats

Security is a complex category that can be interpreted in several ways. It can be seen as a state associated with the absence of threats or as a process involving the continuous activity of actors in the security environment. It can also be viewed as a supreme need, value, and the main purpose of humanity's existence. Security is analyzed in positive terms, as a sense of certainty and a guarantee of protection, as well as in negative terms, as the absence of danger. It is also analyzed in objective terms, referring to the material status of individuals, and in subjective terms, referring to consciousness.[5] Therefore, security should be considered from a multifaceted perspective, given its inherent connection to the conditions of human existence. Security is a fundamental human need, value, and good consisting of two basic elements: ensuring survival and the need for development.[6] Security is the ability to satisfy existential needs and ensure existence, survival, and development.[7]

[3] Silvia Compagnucci, Thomas Osborn, Lorenzo Principali, Domenico Salerno, Daniela Suarato, Romolo Tokong, *L' ecosistema italiano della sicurezza informatica tra regolazione, competitività e consapevolezza* (Roma: I-Com, 2023), 7.

[4] Vittorio Guarriello, "Cybersecurity: una sfida tra pubblica sicurezza e sicurezza nazionale" *Cammino Dritto*, No. 9 (2022): 2.

[5] Andrzej Szczepański, „Pojęcie bezpieczeństwa i jego typologia – próba systematyzacji" *Zeszyty Naukowe Collegium Witelona*, No. 3 (2023): 41. The concept of security is analyzed by, among others: Mirosław Karpiuk, "Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)" *Studia Iuridica Lublinensia*, No. 1 (2019): 191; Krzysztof Kaczmarek, "Wpływ zmian klimatycznych na bezpieczeństwo" *Journal of Modern Science*, No. 4 (2024): 412.

[6] Leszek Goździewski, "Bezpieczeństwo – definicje i jego istota" *Journal of Modern Science*, No. 4 (2024): 363.

[7] Remigiusz Rosicki, "O pojęciu i istocie bezpieczeństwa" *Przegląd Politologiczny*, No. 3 (2010): 24.

Security is an ongoing process. In cyberspace, there are many threats to security – not only to individual IT systems and networks, but also to the entire structure of the modern state. The expanding influence of technology is causing the digitization of all spheres of life.[8] While this brings great convenience, it also poses a significant risk if prudence and skill are lacking when using cyberspace. This threat applies not only to individuals but also to large entities, including businesses. It can harm the functioning and stability of the state.

In the field of security, there is a distinction between cybersecurity, which deals with threats in cyberspace, and other types of security. According to the European Union legislator, cybersecurity means activities necessary to protect networks, information systems, and their users from cyberthreats.[9] Cybersecurity refers to the resilience of information systems against actions that violate the confidentiality, integrity, availability, or authenticity of processed data or services offered by these systems.[10]

[8] Kuba Wojnicki, "Cyberzagrożenia w aspekcie bezpieczeństwa narodowego," [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski (Gdynia: Wydawnictwo BP, 2021): 222.

[9] Art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Dz.Urz.UE z 2019 r., L. 151, s. 15-69). The concept of cybersecurity is analyzed by, among others: Daniele Piva, "Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up" *Corporate Governance Magazine*, No. 4 (2022): 525-538; Małgorzata Czuryk, „Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 44-45; Jarosław Kostrubiec, Mirosław Karpiuk, Dominik Tyrawa, "The status of municipal government in the sphere of ecological security" *Hungarian Journal of Legal Studies*, No. 2 (2024): 175; Jakub Zambrowski, "Incydenty w cyberprzestrzeni," [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski (Gdynia: Wydawnictwo BP, 2021): 228-229; Małgorzata Czuryk, "Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 33-34. Ewa Maria Włodyka, „Cyberbezpieczeństwo sektora publicznego," [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warszawa: ASzWoj, 2024): 66-67. Giovanni Barbara, „La cybersecurity: minacce, evoluzione normativa, corporate governance e nuove prospettive" *Corporate Governance Magazine*, No. 4 (2022): 501-524.

[10] Art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r., poz. 1077 ze zm.). For cybersecurity, see also: Claudio Melchior, Antonella Pococco, Nicola Strizzolo, *La comunicazione eclettica. Le dimensioni comunicative nella web society* (Milano: Franco Angeli, 2020); Tommaso Sica, „Cybersecurity e governo del rischio" *Corporate Governance Magazine*,

Cybersecurity is defined as the protection of systems, networks, and data in cyberspace, where cyberspace is an interactive domain for storing, modifying, and communicating.[11] It is a category aimed at increasing public safety.[12]

Cybersecurity is not a one-dimensional phenomenon. Given its relevance to the information society, a multifaceted approach is required that takes into account the international situation, IT infrastructure, digital competencies, and many other factors that are directly or indirectly related to the security environment.[13]

Security in cyberspace is a necessary part of scientific and technological progress. It determines the need for protection, not only from the point of view of usability, but also to counter completely unknown threats. In the era of global informatization, including of the public sphere, under the conditions of the development of social networks, messages sent to many e-mail addresses, accumulated in big databases – there are often unauthorized actions that may constitute a violation of personal rights, property rights or consumer rights. However, cyberthreats affecting public power structures and the state itself are also becoming more common. As the zone of human privacy free from third-party interference shrinks, the process of informatics affects every sphere of life, including the economy.[14]

By ensuring an adequate level of cybersecurity, uninterrupted social communication is possible, the flow of information is not unduly restricted, individual sectors of the economy (including those of strategic importance) can operate properly. Cybersecurity enables the state to function

No. 4 (2022): 581-594; *Sicurezza Digitale: Sfide e Strategie e Nuove Tecnologie*. https://www.ictsecuritymagazine.com/articoli/sicurezza-digitale/, [accessed: 21.7.2025]; Maddalena Rabitti, Susanna Sandulli, „L'assicurabilità del rischio cibernetico" *Corporate Governance Magazine*, No. 4 (2022): 539-552; *Cybersecurity: le (troppe) lacune che l'Italia deve colmare*. https://www.agendadigitale.eu/sicurezza/cybersecurity--le-troppe-lacune-che-litalia-deve-colmare/. [accessed: 21.7.2025].

[11] Francesca Romana Parente, *Fondamenti di cyber security per tutti* (Roma: Sigma Consulting, 2022): 3.

[12] Anna Makuch, Nicola Strizzolo, „The Social Dimension of Cybersecurity in the Public Media Systems of Poland and Italy" *Cybersecurity and Law*, No. 1 (2024): 211.

[13] Krzysztof Kaczmarek, Mirosław Karpiuk, Claudio Melchior, „A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 105-106.

[14] Katarzyna Chałubińska-Jentkiewicz, „Cyberbezpieczeństwo – zagadnienia definicyjne" *Cybersecurity and Law*, No. 1 (2025): 5-6.

normally.[15] However, in the information age of rapid technical and technological development, it is important to remember that while the internet increases our everyday comfort and convenience, it also exposes us to new threats in the entirely man-made sphere of cyberspace.[16]

It's important to remember that the meaning of digital security has changed significantly in just a few years. A global world connected by digital networks, where states and businesses provide services or implement new technologies and protect rights using digital tools, is a world that is inevitably exposed to growing risks.[17]

IT systems streamline the execution of tasks and allow for the reduction of implementation costs or the reaching of a wider audience in a relatively short time.[18] However, it is important to maintain good cyber hygiene, as this is the only way to minimize the risk of cybersecurity incidents.

Ensuring security is a fundamental task for both countries and international structures. Due to the development of new technologies and the use of cyberspace to provide many services, crises can be triggered by cyberthreats, which are highly dynamic and varied. Because of the intensity of cyberthreats, especially in strategic areas of state activity and important economic sectors, crisis management in the cybersecurity environment requires special attention.[19] Each European Union member state has been required to adopt a national plan for responding to large-scale cybersecurity incidents and crises. This plan must define the objectives and modalities of large-scale cybersecurity incident and crisis management.[20]

[15] Mirosław Karpiuk, „The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 190.

[16] Kacper Pirch, „Socjotechnika jako cyberzagrożenie" [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski (Gdynia: Wydawnictwo BP, 2021): 182.

[17] Andrea Venanzoni, "L'ordine costituzionale della cybersecurity" *Forum di Quaderni Costituzionali Rassegna*, No. 4 (2024): 34.

[18] Mirosław Karpiuk, Claudio Melchior, Urszula Soler, „Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4 (2023): 8.

[19] Małgorzata Czuryk, „Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa" *Ius et Securitas*, No. 1 (2025): 6.

[20] Art. 9 ust. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.Urz.UE z 2022 r., L 333, s. 80-152).

Given the need to ensure the security of core public, economic and social activities, it is crucial to adequately protect critical infrastructure from cyberattacks. According to the European Union legislature, critical infrastructure is defined as a component, facility, equipment, network, or system – or a part thereof – necessary for the provision of a key service. A key service, in turn, is a service that is essential to maintaining social functions, economic activities, health, public safety, and the environment.[21] Critical infrastructure includes the following systems: 1) energy supply, energy resources, and fuels; 2) communications; 3) IT networks; 4) finance; 5) food supply; 6) water supply; 7) healthcare; 8) transportation; 9) rescue services; 10) the continuity of public administration; and 11) the production, storage, and use of chemicals and radioactive substances, including hazardous substance pipelines.[22] Of particular importance in this regard is the power grid, which uses IT systems.

The power grid and the IT network are increasingly interdependent. The former is managed by the latter, which it also powers. The collapse of one inevitably causes the collapse of the other, creating a cycle of mutual vulnerability. Smart grids, defined as integrated systems for managing information and controlling energy flows from production to the end consumer, represent a significant technological innovation but also a prime target for cyberattacks.

The consequences of an attack on a smart grid would be catastrophic, with millions of interconnected devices affected immediately and on a large scale. It is no coincidence that numerous recent scientific publications have highlighted the risks associated with this interconnection, emphasizing the importance of international collaboration to prevent both physical and cyberattacks.[23]

The critical infrastructure is computerized and consists of systems that are responsible for the proper functioning of the most important sectors in the state. These systems are closely interconnected and vulnerable to attacks. Damage or interruption to one system can affect the others, so

[21] Art. 2 pkt 4-5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.Urz.UE z 2022 r., L 333, s. 164-198).

[22] Art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r., poz. 122 ze zm.).

[23] *Threat Landscape*, https://www.enisa.europa.eu/publications, [accessed: 18.05.2025]; *Global Risk Report 2022*. https://www.weforum.org/reports. [accessed: 18.05.2025].

securing them is crucial for the state's economy. Methods to protect these systems must be improved continuously to ensure their continuity, functionality, and integrity. However, security's role is only to minimize risk because complete elimination is impossible due to many factors.[24]

3 | Artificial intelligence and security in cyberspace

Digitization is of particular importance when it comes to technological evolution, enabling the transformation of traditional methods of work, communication, and access to information. This process, which involves transferring data and services to the virtual space, has become the foundation of modern societies. It involves transferring data and services to the virtual space, has become the foundation of modern societies. Through the implementation of advanced technologies, such as artificial intelligence, digitization contributes to the automation and optimization of processes in various sectors, ranging from industry to public services. These changes directly impact the daily lives of citizens and the efficiency of the state. Additionally, the development of communication technologies eliminates geographic and social barriers, enabling greater global integration.[25]

Artificial intelligence is defined as a machine system designed to operate at different levels of autonomy and adaptability, and it can infer how to generate results that can affect reality or a virtual area based on the input received.[26] Artificial intelligence includes any software or hardware

[24] Kuba Wojnicki, "Cyberzagrożenia w aspekcie bezpieczeństwa narodowego," [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski (Gdynia: Wydawnictwo BP, 2021): 211.

[25] Tomasz Wojciechowski, "Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego" *Ius et Securitas*, No. 1 (2024): 84.

[26] Art. 3 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Dz.Urz.UE z 2024 r., L 2024/1689).

component that supports machine learning, computer vision, natural language processing and generation, and robotics.[27]

The risks associated with artificial intelligence systems apply to their design and use. At both stages, due diligence is required to minimize these risks as much as possible.[28]

In order to mitigate the risks associated with AI, a multidimensional approach is essential. Wojciech Mazurczyk et al. suggest that a "layered approach" may be the most effective method of dealing with this type of threat in a "holistic manner".[29] In order to implement effective long-term solutions, it is vital to raise awareness, improve media literacy, encourage stakeholder cooperation and establish clear regulations. The European Union has stated that effective long-term solutions require awareness-raising, more media literacy, broad stakeholder involvement.[30] In the absence of a concerted response, the potential of AI to be a double-edged sword, capable of both societal destabilisation and protection, is a matter of significant concern.

It is evident that artificial intelligence (AI) has the potential to transform the information landscape; however, the extent of its impact is contingent upon the manner in which it is managed. This challenge is not solely technological in nature; it is also social, political and ethical. To ensure that AI becomes a catalyst for progress and security, it is imperative to promote responsible innovation, enhance detection and prevention capabilities, and ensure that technologies are utilized for the benefit of society as a whole.

Artificial intelligence can have both positive and negative effects on society. The main disadvantage of artificial intelligence is that it can be used to conduct an effective disinformation process. This is related to its ability to manipulate society.[31] Despite the advantages of AI and the improvements it has made, this technology should be used with caution.

[27] Krzysztof Kaczmarek, "Sztuczna inteligencja," [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warszawa: ASzWoj, 2024): 251-252.

[28] Dominik Bierecki, Christophe Gaie, Mirosław Karpiuk, "Artificial Intelligence in e-Administration" *Prawo i Więź*, No. 1 (2025): 403.

[29] Wojciech Mazurczyk, Dongwon Lee, Andreas Vlachos, "Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective" *Communications of the ACM*, No. 3 (2024): 36-39.

[30] *Tackling online disinformation: A European approach. Communication COM(2018) 236 final.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236. [accessed: 30.1.2025].

[31] Tomasz Gergelewicz, „Bipolarity of Artificial Intelligence – Chances and Threats" *Ius et Securitas*, No. 2 (2024): 72-73.

Artificial intelligence learns from large amounts of data, but sometimes the data is not diverse enough.[32]

Artificial intelligence algorithms significantly outperform humans in their ability to identify patterns and analyze data. This, in turn, enhances the ability to create specific concepts and make decisions.[33] Artificial intelligence is undoubtedly a technology that drives many spheres of human existence. However, it can also be used as a tool of information attack against society and the state. This technological discovery is a double-edged sword that, on the one hand, offers great opportunities for civilizational development and, on the other hand, poses threats to human cognition and recognition of reality.[34]

Artificial intelligence is an extremely useful tool that offers new opportunities in many industries. However, it is important to remember that it's not a solution to every problem. In fact, it can cause more harm than good. Using artificial intelligence consciously allows you to seamlessly work with any tool based on it. In the right hands, working with AI can be highly convenient, though its drawbacks should always be kept in mind.[35]

The development determined by new technologies is based, among other things, on the recognition that artificial intelligence can automate routine activities, allowing to focus on complex, strategic activities.[36] This eases the burden on individuals using artificial intelligence systems for low-risk tasks. However, artificial intelligence can also be helpful in undertaking complex activities, provided that humans do not trust it unreservedly and remain critical of the results it generates.

[32] Piotr Zaborowski, "Sztuczna inteligencja – wątpliwości, pułapki i obawy" *Cybersecurity and Law*, No. 1 (2025): 151.

[33] Kazimierz Pawelec, „Zwyczaj w ruchu drogowym i jego identyfikacja" *Ius et Securitas*, No. 1 (2025): 70.

[34] Tomasz Gergelewicz, „Sztuczna inteligencja w perspektywie zagrożeń informacyjnych" *Przegląd Sił Zbrojnych*, No. 2 (2025): 146.

[35] Piotr Zaborowski, "Sztuczna inteligencja – wątpliwości, pułapki i obawy" *Cybersecurity and Law*, No. 1 (2025): 152.

[36] András Bencsik, "The Opportunities of Digitalisation in Public Administration with a Special Focus on the Use of Artificial Intelligence" *Studia Iuridica Lublinensia*, No. 2 (2024): 21.

4 Conclusion

The position of data entities in cyberspace is largely determined by the information and communication technologies at their disposal.[37] Their purchase, servicing and updating are costly, and therefore cybersecurity is being spared by not introducing new solutions in this area, with the result that the vulnerability of IT systems to cyberattacks is increasing over the years (or even months), posing a high risk of cybersecurity incidents.

It should be remembered that any new technology can be both convenient and risky. In today's era of cultural and social changes and technological development, it is difficult to live without the internet. However, a lack of caution when using it creates the risk of cyberattacks, cyberbullying, image exploitation, and phishing. An infected network can put servers and connected devices out of service.[38]

Facing the challenges posed by the development of new technologies, today's society must adapt to changing conditions while maintaining its cultural identity. Achieving sustainable development and social stability requires integrated actions in technology, social policy, and culture.[39]

Due to the high threat level posed by cyber incidents, an adequate level of cybersecurity must be maintained.[40] The European Union and international structures must be involved in ensuring protection against cyber threats. Along with introducing appropriate technical requirements, legal solutions adequate to the threats must be adopted. It is also important to note the protection of human freedoms and rights, which are often violated in cyberspace Prosecuting these violations is difficult due to the perpetrators' high level of anonymity.

Finally, it should be emphasized that we live in a world where media and new technologies significantly impact the way modern societies function. We can communicate more easily, access information, and have greater access to knowledge. At the same time, however, we must recognize

[37] Christophe Gaie, Mirosław Karpiuk, Nicola Strizzolo, "Cybersecurity of Public Sector Institutions" *Prawo i Więź*, No.6 (2024): 359.

[38] Bogdan Grabowski, "Cyfrowe zagrożenia – zarys problemu" *Ius et Securitas*, No. 1 (2024): 103.

[39] Dagmara Cholewińska, "Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia" *Ius et Securitas*, No. 1 (2025): 51.

[40] Jakub Zambrowski, "Incydenty w cyberprzestrzeni", [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski (Gdynia: Wydawnictwo BP, 2021): 244.

the problems associated with modern technological advances. For example, communication via the internet has changed the nature of traditional threats. We are witnessing the emergence of new social pathologies and dysfunctions, particularly social ones.[41] We should also not forget about preserving human dignity in a digital society.[42]

Bibliography

Barbara Giovanni, "La cybersecurity: minacce, evoluzione normativa, corporate governance e nuove prospettive" *Corporate Governance Magazine*, No. 4 (2022): 501-524.

Bencsik Andras, "The Opportunities of Digitalisation in Public Administration with a Special Focus on the Use of Artificial Intelligence" *Studia Iuridica Lublinensia*, No. 2 (2024): 11-23.

Bierecki Dominik, Gaie Christophe, Karpiuk Mirosław, "Artificial Intelligence in e-Administration" *Prawo i Więź*, No. 1 (2025): 383-407.

Carpegna Brivio Elena, "Punteggi reputazionali e dignità nella società digitale", [in:] *La reputazione nell'era digitale. Rappresentazioni e pratiche del sé tra capitale sociale e bene relazionale*, ed. Eleonora Sparano, Nicola Strizzolo, Martina Lippolis. 235-260. Roma: Eurilink University Press, 2024.

Chałubińska-Jentkiewicz Katarzyna, „Cyberbezpieczeństwo – zagadnienia definicyjne" *Cybersecurity and Law*, No. 1 (2025): 1-24.

Cholewińska Dagmara, "Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia" *Ius et Securitas*, No. 1 (2025): 41-52.

Compagnucci Silvia, Thomas Osborn, Lorenzo Principali, Domenico Salerno, Daniela Suarato, Romolo Tokong, *L' ecosistema italiano della sicurezza informatica tra regolazione, competitività e consapevolezza*. Roma: I-Com, 2023.

Czuryk Małgorzata, "Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 43-52.

[41] Andrzej Pieczywok, "Wirtualna przestrzeń edukacji człowieka" *Ius et Securitas*, No. 1 (2025): 53.

[42] Elena Carpegna Brivio, "Punteggi reputazionali e dignità nella società digitale", [in:] *La reputazione nell'era digitale. Rappresentazioni e pratiche del sé tra capitale sociale e bene relazionale*, ed. Eleonora Sparano, Nicola Strizzolo, Martina Lippolis (Roma: Eurilink University Press, 2024), 235-260.

Czuryk Małgorzata, "Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 31-43.

Czuryk Małgorzata, "Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa" *Ius et Securitas*, No. 1 (2025): 5-12.

Gaie Christophe, Mirosław Karpiuk, Nicola Strizzolo, "Cybersecurity of Public Sector Institutions" *Prawo i Więź*, No.6 (2024): 347-362.

Gergelewicz Tomasz, "Bipolarity of Artificial Intelligence – Chances and Threats" *Ius et Securitas*, No. 2 (2024): 7194.

Gergelewicz Tomasz, "Sztuczna inteligencja w perspektywie zagrożeń informacyjnych" *Przegląd Sił Zbrojnych*, No. 2 (2025): 143-146.

Goździewski Leszek, "Bezpieczeństwo – definicje i jego istota" *Journal of Modern Science*, No. 4 (2024): 356-374.

Grabowski Bogdan, "Cyfrowe zagrożenia – zarys problemu" *Ius et Securitas*, No. 1 (2024): 95-105.

Guarriello Vittorio, "Cybersecurity: una sfida tra pubblica sicurezza e sicurezza nazionale" *Cammino Dritto*, No. 9 (2022): 1-19.

Kaczmarek Krzysztof, "Sztuczna inteligencja," [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz. 250-252. Warszawa: ASzWoj, 2024.

Kaczmarek Krzysztof, "Wpływ zmian klimatycznych na bezpieczeństwo" *Journal of Modern Science*, No. 4 (2024): 410-430.

Kaczmarek Krzysztof, Mirosław Karpiuk, Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 103-121.

Karpiuk Mirosław, "Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)" *Studia Iuridica Lublinensia*, No. 1 (2019): 185-194.

Karpiuk Mirosław, "Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź*, No. 4 (2022): 166-179.

Karpiuk Mirosław, "The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 190.

Karpiuk Mirosław, Claudio Melchior, Urszula Soler, "Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4 (2023): 7-27.

Kostrubiec Jarosław, Mirosław Karpiuk, Dominik Tyrawa, "The status of municipal government in the sphere of ecological security" *Hungarian Journal of Legal Studies*, No. 2 (2024): 164-181.

Makuch Anna, Nicola Strizzolo, "The Social Dimension of Cybersecurity in the Public Media Systems of Poland and Italy" *Cybersecurity and Law*, No. 1 (2024): 200-212.

Mazurczyk Wojciech, Dongwon Lee, Andreas Vlachos, "Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective" *Communications of the ACM*" No. 3 (2024): 36-39.

Melchior Claudio, Antonella Pococco, Nicola Strizzolo, *La comunicazione eclettica. Le dimensioni comunicative nella web society*. Milano: Franco Angeli, 2020.

Parente Francesca Romana, *Fondamenti di cyber security per tutti*. Roma: Sigma Consulting, 2022.

Pawelec Kazimierz, "Zwyczaj w ruchu drogowym i jego identyfikacja" *Ius et Securitas*, No. 1 (2025): 65-73.

Pieczywok Andrzej, "Wirtualna przestrzeń edukacji człowieka" *Ius et Securitas*, No. 1 (2025): 53-65.

Pirch Kacper, "Socjotechnika jako cyberzagrożenie," [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski. 191-202. Gdynia: Wydawnictwo BP, 2021.

Piva Daniele, "Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up" *Corporate Governance Magazine*, No. 4 (2022): 525-538.

Rabitti Maddalena, Susanna Sandulli, „L'assicurabilità del rischio cibernetico" *Corporate Governance Magazine*, No. 4 (2022): 539-552.

Rosicki Remigiusz, "O pojęciu i istocie bezpieczeństwa" *Przegląd Politologiczny*, No. 3 (2010): 23-32.

Sica Tommaso, „Cybersecurity e governo del rischio" *Corporate Governance Magazine*, No. 4 (2022): 581-594.

Szczepański Andrzej, „Pojęcie bezpieczeństwa i jego typologia – próba systematyzacji" *Zeszyty Naukowe Collegium Witelona*, No. 3 (2023): 27-44.

Venanzoni Andrea, "L'ordine costituzionale della cybersecurity" *Forum di Quaderni Costituzionali Rassegna*, No. 4 (2024): 33-80.

Włodyka Ewa Maria, "Cyberbezpieczeństwo sektora publicznego", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz. 64-67. Warszawa: ASzWoj, 2024.

Wojciechowski Tomasz, "Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego" *Ius et Securitas*, No. 1 (2024): 83-94.

Wojnicki Kuba, "Cyberzagrożenia w aspekcie bezpieczeństwa narodowego," [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski. 203-224. Gdynia: Wydawnictwo BP, 2021.

Zaborowski Piotr, "Sztuczna inteligencja – wątpliwości, pułapki i obawy" *Cybersecurity and Law*, No. 1 (2025): 147-153.

Zambrowski Jakub, "Incydenty w cyberprzestrzeni", [in:] *Cyberbezpieczeństwo. Teoretycznie i empirycznie w naukach o bezpieczeństwie*, ed. Robert Adam Janczewski. 226-246. Gdynia: Wydawnictwo BP, 2021.