CHRISTOPHE GAIE, MIROSŁAW KARPIUK, NICOLA STRIZZOLO

Cybersecurity of Public Sector Institutions

Abstract

In the information society, the public sector must anticipate needs related to the ever-present use of cyberspace for providing services. On the one hand, new technologies facilitate and streamline the fulfillment of public tasks, and on the other hand, they pose threats that might produce far-reaching consequences. This means that public entities are obliged to apply solutions adequate to potential threats. As information and communication technology (ICT) systems being used by public sector institutions should operate uninterruptedly, it is necessary to implement measures to ensure such systems' resilience to cyberattacks. Artificial intelligence (AI) might prove helpful for ensuring cybersecurity. However, this technology should be used with caution to prevent damage to the public sector resulting from its improper use. The research methods used in this paper include both the law theory method and the doctrinal legal research method. These methods were applied to analyze the literature on the subject and legal texts from the perspective of cybersecurity in the public sector. The paper also emphasizes the necessity of considering evolving cybersecurity frameworks that account for the global nature of cyberthreats, as well as the unique challenges faced by public institutions in balancing efficiency with security needs.

KEYWORDS: cybersecurity, public sector, cyberspace

CHRISTOPHE GAIE – PhD in telecomunications, Ministry of Public Transformation, France, ORCID – 0000-0002-8252-5278, e-mail: christophe.gaie@gmail.com
MIROSŁAW KARPIUK – professor in law, University of Warmia and Mazury in Olsztyn, Poland, ORCID – 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl
NICOLA STRIZZOLO – associate professor, University of Teramo, Italy, ORCID – 0000-0001-6384-9210, e-mail: nstrizzolo@unite.it

HTTPS://DOI.ORG/10.36128/PRIW.VI53.1129

1 | Introduction

To a large extent, the public sector relies on ICT systems intended not only for conducting its day-to-day office operations but also for performing tasks (including strategic ones) and providing services to individuals, social groups, and the entire society. As it was necessary to universally computerize public administration, facilitate access to a public office, accelerate case-handling procedures and reduce operational costs, ensuring the security of the ICT systems used by the administration became paramount. Turning to new technologies, the public sector must, at the same time, take due care of cybersecurity. Cyberspace is exposed to a great number of threats such as detailed by the European Union Agency for Cybersecurity (ENISA)[1]. Therefore, the public sector needs to take this fact into account while operating in cyberspace and to appropriately protect activities conducted there. As the public sector increasingly relies on digital tools, its vulnerability of the public sector to cyberattacks is growing, making the development of robust cybersecurity frameworks more critical than ever[2]. As digital transformation accelerates across all levels of government, it is imperative to ensure that emerging cyber threats do not compromise the integrity of digital and traditional public services.

The mission of public sector institutions is to effectively meet social needs, both at the local, regional, and national levels, as well as on a global scale. These institutions increasingly often perform the work they have been assigned using ICT systems, which make the provision of public tasks more efficient as well as allow them to reduce costs and reach a wider group of addressees in a relatively short time. As the public sector is a factor that not only stimulates the process of providing social services but also compels process users to act in a specified way, proper management in this sphere is becoming increasingly important (cybersecurity management included). Public institutions not only provide services to society but also undertake measures related to the sphere of exercising certain powers (public administration). They shape the citizen status within the state and

[1] ENISA, *ENISA Threat Landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. [accessed: 18.11.2024].

[2] Berndt Writz, Jan Weyerer, „Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats” *International Journal of Public Administration*, No. 40 (2016).

influence the economic sphere[3]. The complexity of modern governance demands that public sector institutions not only provide services efficiently but also maintain trust. Indeed, citizens may lose trust in public services if institutions neglect to build a robust cybersecurity ecosystem[4].

It should be noted that the social awareness of threats related to the improper use of digital tools is insufficient, which is why they should not be neglected, as this might give rise to some serious consequences[5]. Public institutions must take this into account when providing services by electronic means. A vast share of threats arising from violating cybersecurity rules can be attributed to the addressees of public services, as such breaches might disrupt the normal operation of ICT systems used by public institutions, even resulting in the paralysis of these entities in extreme cases. These attacks are escalating due to several factors: AI-generated viruses and malware can easily steal money from public service users, adversarial countries aim to paralyze government administrations by denying public services, and hacktivists seek to gain attention by disrupting public services[6].

The paper's objective is to analyze public institution activities from the perspective of cybersecurity. In a state where the public sector is largely digitized and a significant portion of its tasks are conducted using cyberspace, the security of ICT systems should be prioritized. Disruptions in the provision of e-services might undermine society's trust in public administration and the entire state, which is obligated to act for its citizens, particularly to meet the needs of an information society. Ensuring reliable public services in today's complex digital landscape requires robust infrastructure, clear policy frameworks, and continuous investment in cybersecurity to stay ahead of emerging threats. By staying ahead of emerging

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

[4] Shahrin Sadik, Mohiuddin Ahmed, Leslie Sikos, Najmul Islam, „Toward a Sustainable Cybersecurity Ecosystem" *Computers*, No. 9 (2020).

[5] Krzysztof Kaczmarek, „Etyka a prawo w edukacji", [in:] *Prawo w poszukiwaniu prawdy, dobra i piękna. Księga Jubileuszowa ks. prof. Sławomira Fundowicza*, ed. Paweł Śwital, Bartosz Kuś, Emilia Gulińska (Radom: Wydawnictwo Naukowe, 2024), 481.

[6] Tahsin Hossain, Tan Yigitcanlar, Kien Nguyen, Yue Xu, „Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework" *Applied Sciences*, No. 13: (2024): 5501.

threats, governments can maintain the security and functionality of their IT systems, fostering citizen trust and adoption[7].

An analysis of the literature on the subject was performed to study the cybersecurity of public sector institutions. This allowed the definition of the theoretical grounds that determine the status of public institutions in the cybersecurity sphere. In using the doctrinal legal research method, emphasis was placed on the normative aspects of protecting public institutions against cyberthreats. The primary research problem is expressed in a question about the effectiveness of protecting the public sector's ICT systems against cyberthreats, particularly when it comes to the legal safeguards of such protection.

2 | Cyberspace as a sphere of public operations

Cyberspace is a communication space facilitated by internet link systems. It allows its users to communicate online and establish relationships in real time. Cyberspace is an environment for information exchange via computer networks and systems. It is also a sphere of activity where all actions differ in nature from those pursued in the physical environment. Alongside the land, maritime, air and outer-space environments, including military activities, alongside the land, maritime, air, and outer-space environments[8]. According to the legal definition, cyberspace is understood as a space for processing and exchanging information created by ICT systems, including the links between them and their relations with users[9].

Kellerman defines four imbricated concepts: 1) virtual space, the overarching dimension encompassing both digital and physical representations of real-world spaces, 2) cyberspace, which focuses on digital communication and information media and refers to digital spaces accessed through

[7] Shahrukh Mushtaq, Shah Mahmood, „Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management" *Information*, No. 10 (2024): 619; Mengzhong Zhang, Manpreet Kaur, „Toward a theory of e-government: Challenges and opportunities, a literature review" *Journal of Infrastructure, Policy and Development*, No. 10 (2024): 7707.

[8] Maciej Marczyk, „Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru" *Przegląd Teleinformatyczny*, No. 1-2 (2018): 59.

[9] Article 2(1a) of the Martial Law Act of 21 June 2002 (t.j. Dz.U. z 2017 r., poz. 1928).

the Internet, 3) the Internet, a specific subset of cyberspace, a global network of interconnected computers facilitating communication and information exchange, and 4) Internet screen-space (ISS), which refers to the visual interface users have with the Internet[10].

Cyberspace generates new threats and compels humans to face other, previously unknown, challenges. It redefines the sphere of security and creates new risk parameters. It also contributes to transforming lifestyles and defines approaches, behaviours and actions we undertake. Contemporary human problems related to the use of cyberspace are currently present in practically all spheres of our lives (private, professional and public), and they are not limited to specific threats only but extend across the entirety of human existence. New threats and related risk factors produce the need to respond adequately, with the specific nature of changes taking place in mind[11]. Public institutions, obliged to meet societal needs, must also keep pace with the rapid civilisation transformations related to new technologies and adapt their operations to the challenges of contemporary times. The current context exposes government IT systems to a multitude of evolving threats, including information manipulation for political violence such as the attacks on the US Capitol in 2021 and on Brazil's Congress in January 2023. The use of social media platforms like X may be exploited to disseminate disinformation, as observed during riots in the UK in 2024[12].

New current cyberthreats also include data theft for criminal activities and requires establishing strong cybersecurity measures. These incidents highlight the importance of establishing strong cybersecurity measures to protect sensitive information[13]. For example, the Dutch organ donor

[10] Aharon Kellerman, *Geographic Interpretations of the Internet* (Cham: Springer, 2016).

[11] Krzysztof Drabik, „Cyberprzestrzeń – zagrożenia i wyzwania", [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. Mirosław Karpiuk (Warszawa: ASzWoj, 2024), 7.

[12] Naja Bentzen, „Online information manipulation and information integrity: An overview of key challenges, actors and the EU's evolving response". https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762416. [accessed: 18.11.2024].

[13] Seumas Miller, Terry Bossomaier, „Cybersecurity: Threats, Countermeasures, and the Institutional Landscape", [in:] *Cybersecurity, Ethics, and Collective Responsibility*, eds. Seumas Miller, Terry Bossomaier (New York: Oxford Academic, 2024).

breach in March 2020 and the Irish Health Service Executive (HSE) attack I May 2021 are real-world examples of data theft for criminal purposes[14].

Cyberspace is becoming an increasingly effective element of confrontation in both military and non-military spheres. It is attractive to all conflict actors, as it allows the fulfillment of strategic objectives without revealing their identities, which is particularly dangerous to the party under attack. The ongoing advancement in the scientific and technological sphere, where information and communication technologies occupy a prominent position, makes cyberspace a perfect place for acquiring and disrupting information. It is worth remembering that cyberspace and the tools used there constitute a grave threat to humans[15]. Cyberspace is home to a dangerous phenomenon called „information noise". It is a surge of insignificant information that diverts our attention from significant data or diminishes its importance. Information noise is created by presenting recipients with an excess of incomplete, irrelevant, contradictory, or similar information which leads to a situation where the recipients of specified contents lose their ability to differentiate between the things they should focus on from the unimportant ones and to evaluate the weight of individual pieces of information[16]. For example, France's open data platform (https://www.data.gouv.fr/en/) offers a vast collection of public information, encompassing 46,326 datasets and 231,784 files as of November 11th, 2024. This represents terabytes of data, distinct from information protected by professional secrecy.

Disruptions in cyberspace might negatively affect the functioning of the state, which is to ensure the appropriate quality of the services it provides, including services of strategic importance. As it is necessary to secure such services and to ensure their continuity, reach and availability to everyone, it is necessary to adopt measures aimed at their protection against cyberthreats[17]. For instance, Casalegno et al. identified key factors

[14] Kyle Chin, Biggest Data Breaches. https://www.upguard.com/blog/biggest--data-breaches-europe. [accessed: 19.11.2024].

[15] Andrzej Żebrowski, „Cyberprzestrzeń miejscem walki (wojny) informacyjnej (wybrane aspekty)", [in:] *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni*, ed. Joanna Grubicka, Aneta Kamińska-Nawrot (Słupsk: Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, 2020), 9.

[16] Tomasz Gergelewicz, *Informacja sygnalna. Katalog obszarów działań antydezinformacyjnych* (Warszawa: ASzWoj, 2023), 3.

[17] 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.

contributing to public service resilience during crises like the COVID-19 pandemic[18]. These factors, such as contextual awareness, resource availability, decision-making autonomy, collaborative strategies, and digital transformation, can also bolster resilience against security breaches. By prioritizing these areas, public services can enhance their continuity and effectiveness.

3 Ensuring cybersecurity in public entities

In the age of information society and information state, where access to digital services is universal, cybersecurity has gained particular importance because it allows uninterrupted social communication and facilitates proper protection of strategic economy sectors, thus contributing to the enhanced efficiency of public task performance. Cybersecurity ensures protection against threats, thus securing the normal functioning of the state as a public entity at multiple levels[19]. It is essential for safeguarding the core functions of governments. It protects the delivery of critical services such as tax collection, welfare programs, and healthcare, while safeguarding the sensitive personal data of citizens. Moreover, cybersecurity shields state-owned physical and digital assets, including websites, data centers, and government buildings, from cyberattacks. Additionally, it safeguards the critical infrastructure that underpins societal functions, such as communication networks, energy systems, and financial systems, ensuring their resilience against cyber threats.

The EU legislator defines cybersecurity as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyberthreats[20].

[18] Cecilia Casalegno, Chiara Civera, Damiano Cortese, Alessandro Zardini, „In Search of the Enabling Factors for Public Services Resilience: A Multidisciplinary and Configurational Approach" *Journal of Innovation & Knowledge*, No. 1 (2023): 100337. https://doi.org/10.1016/j.jik.2023.100337.

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

[20] Article 2 (1) of the Regulation (EU) 2019/881 of the European Parliament and of the Council of April 17, 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity

Due to the need to ensure cybersecurity, it appears indispensable to adopt a proper approach to protect ICT systems, which means that the level of such protection must be high. Given the obligation to guarantee such a level, in certain circumstances, rights and freedoms vested in individuals might be restricted in cyberspace. Such limitations are permissible only if protection cannot be provided otherwise[21]. Restrictions on exercising human and civil rights and freedoms cannot be introduced automatically, as the nature of the threat must be taken into account in such cases, and the limitations must be proportional to the objective that is to be reached through their deployment[22]. Public authorities should not always prioritise cybersecurity over other interests, particularly the rights and freedoms of individuals. Restrictions are only permissible in circumstances where there are no alternative means to ensure security in cyberspace, and in such cases, cybersecurity should take precedence over these rights.

In situations where cyberattacks could severely disrupt critical public services, exceptional measures might be necessary. This could involve granting extended investigative powers to specialized government agencies, overseen by a designated judicial body. Such measures could be justified when the threat posed by cybercriminals outweighs potential privacy concerns. Collaboration between organizations responsible for critical infrastructure, such as the partnership between Transport for London and the National Crime Agency[23], could be crucial in apprehending cybercriminals, even those as young as seventeen.

certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ EU of 2019, L 151, p. 15). For additional information about the definition of cybersecurity, refer to: Christophe Gaie, Mirosław Karpiuk, „The Provision of e-Services by Public Administration Bodies and Their Cybersecurity", [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, ed. Christophe Gaie, Mayuri Mehta (Cham: Springer, 2024), 183-184; Małgorzata Czuryk, „Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 44-45; Mirosław Karpiuk, Jarosław Kostrubiec, „Provincial Governor as a Body Responsible for Combating State Security Threats" *Studia Iuridica Lublinensia*, No. 1 (2024): 117.

[21] Małgorzata Czuryk, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 34.

[22] Małgorzata Czuryk, „Activities of the Local Government During a State of Natural Disaster" *Studia Iuridica Lublinensia*, No. 4 (2021): 121.

[23] Jefss Warren, *London Transport Cyber Attack: Boy, 17, Arrested*. https://www.bbc.com/news/articles/c4gqg2elkj40. [accessed: 19.11.2024].

The analysis of the significance of cybersecurity for the digital society requires a holistic approach, as part of which, in addition to ICT infrastructure and the level of digital skills, several factors should be taken into consideration, including, for instance, the security environment and international situation[24]. Given the ongoing conflict between Ukraine and Russia, coupled with intense global economic competition, it is prudent to consider foreign nations as potential adversaries beyond the traditional East-West divide. Recent cyberattacks, such as those attributed to China targeting the United States[25] or the United States' support for Ukraine against Russia[26], further underscore the complexity of modern geopolitical tensions.

From the perspective of the public sector, cybersecurity management – or, in other words, risk management in the sphere of cybersecurity – is becoming increasingly important, particularly in emergency situations. In the European Union, each Member State is required to designate or establish at least one competent authority responsible for managing large-scale cybersecurity incidents and crises. Member States are obliged to ensure that such cybercrisis management authorities have adequate resources to carry out the tasks assigned to them, both effectively and efficiently. Cybercrisis management must be coherent with existing frameworks for general national crisis management[27].

Cybersecurity is becoming an essential expectation, the fulfillment of which is a decisive factor in whether the technological revolution will be embraced across society or not[28]. The public sector must meet these expectations by keeping pace with the rapidly changing needs of digitized

[24] 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.

[25] Anders Triay, Robert Legare, Kathryn Watson, *The U.S. Is Investigating a China-Backed Hack of Telecom Companies. Here's What to Know*. https://www.cbsnews.com/news/us-investigating-hack-major-telecom-companies-by-china/, [accessed: 20.11.2024].

[26] Joe Tidy, *Why Is It so Rare to Hear about Western Cyber-Attacks?*. https://www.bbc.com/news/technology-65977742, [accessed: 20.11.2024].

[27] Article 9 (1) of 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) (OJ EU of 2022, L 333, p. 80-152).

[28] Krzysztof Gawkowski, „Cyberbezpieczeństwo w inteligentnym mieście" *Cybersecurity and Law*, No. 2 (2023): 103.

societies, for which cyberspace is where individual society members carry out activities in most areas of their lives. Integrating security into the entire lifecycle of digital projects is paramount. Adopting DevSecOps principles enables IT teams to enhance their cybersecurity skills and prioritize the protection of every ICT component, including software, systems, infrastructure, networks, and data[29]. This approach fosters a proactive security culture, ensuring that cybersecurity is considered from the initial stages of development to the final deployment and maintenance phases.

Artificial intelligence systems might be of great assistance in identifying and combating cyberattacks in the public sector, especially when dealing with technological progress. Not only can artificial intelligence make the operations of public entities more effective and less costly, but it can also improve security in cyberspace, where such institutions provide their services. If applied properly, artificial intelligence, as a technology of the future, might predict, neutralize, and prevent cyberthreats despite their diversity and dynamics. However, as we should bear in mind that AI might have its share in the emergence of such threats, it needs to be used responsibly, and the risk-benefit trade-off must be carefully assessed[30]. Indeed, AI's ability to quickly analyze massive datasets and identify patterns makes it a powerful tool for cybersecurity. Its self-learning capability allows it to adapt to evolving threats. However, careful management is crucial to prevent the introduction of new vulnerabilities, biases, or ethical concerns. It is also essential to safeguard AI systems from malicious actors who might manipulate training data or exploit interactive components to deceive public service users.

An increasing number of decisions within institutions, as well as in the provision of services, are being delegated to artificial intelligence (AI) systems.

While AI can reduce costs (although these savings may translate into social costs associated with the displacement of human labor) and minimize errors, it can also scale cultural biases embedded by programmers

[29] Arun Sandu, „DevSecOps: Integrating Security into the DevOps Lifecycle for Enhanced Resilience" *Technology & Management Review*, No. 6 (2021).

[30] Dinesh Kalla, Sivaraju Kuraku, Fnu Samaah, *Advantages, Disadvantages and Risks Associated with ChatGPT and AI on Cybersecurity*. https://ssrn.com/abstract=4619204. [accessed: 18.11.2024].

who may lack an understanding of the social realities of the intended users. This can lead to the perpetuation of social injustices on a large scale[31].

For instance, in the United States, healthcare algorithms have been found to discriminate against ethnic minorities, leading to the allocation of fewer resources to these groups compared to other social demographics[32]. In another case, numerous prisoners were held in custody longer than necessary due to algorithmic decisions[33].

An additional risk arises when not only traditional digital systems but also AI systems responsible for critical decisions become vulnerable. Hacking into an AI system that governs critical infrastructures can have catastrophic consequences, negatively impacting essential services such as energy, healthcare, and public safety.

4 | Conclusions

The state should engage in the development of an information society and, as such, in the protection of cybersecurity through the development of information technologies within public administration itself, in the sphere of its contacts with citizens, and with respect to state investments in ICT infrastructure. These measures should be aimed at addressing issues that are related to the sphere in question. The following activities should be noted: eliminating digital exclusion, protecting consumers in e-commerce, combating computer crime, developing electronic payment systems, respecting the individual privacy, and protecting intellectual property rights[34]. Developing a robust cybersecurity strategy is essential to harness

[31] Nicola Strizzolo, Eleonora Sparano, „Inconsapevolezza Artificiale. Dalla fiducia alla fede nelle macchine" *Sociologia. Rivista Quadrimestrale di Scienze Sociologiche, Storiche e Giuridiche*, No. 3 (2024): 6-7.

[32] Ziad Obermeyer, Brian Powers, Christine Vogeli, Sendhil Mullainathan, "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations" *Science*, No. 6464 (2019): 447-453.

[33] Nicola Strizzolo, *Smart grid, i pericoli di una rete energetica connessa*. https://www.agendadigitale.eu/sicurezza/smart-grid-i-pericoli-di-una-rete-energetica-connessa/. [accessed: 18.11.2024].

[34] Dominik Tyrawa, „Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane" *International Journal of Legal Studies*, No. 1 (2023): 19.

the benefits of digitization without compromising public trust or security. By prioritizing security from the outset and adopting innovative approaches like DevSecOps, policymakers can ensure that digital projects are secure by design. This proactive approach will help safeguard critical infrastructure, protect sensitive data, and mitigate cyber threats, ultimately fostering a secure digital future.

It should be stressed that it is impossible to fully eliminate threats in cyberspace. However, there are two key non-technical ways to mitigate vulnerability: education and universal awareness of such risks. This pertains to the whole society and all types of activities in cyberspace (including in the public sphere). For such education measures to yield the expected results, it is crucial to raise the level of digital skills acquired by persons responsible for education in this respect. This issue becomes even more important in view of the fact that the widespread access to the Internet and technology development might contribute to the evolution of existing hazards or to the emergence of new, previously unknown threats[35]. Integrating cybersecurity education into both initial academic programs and ongoing professional development is crucial. By leveraging specialized services that understand the unique challenges of secure government service development, IT professionals can acquire and maintain the necessary skills to build robust and resilient systems. This continuous learning approach ensures that professionals stay up-to-date with the latest threats and best practices in cybersecurity.

In the area of cybersecurity, proposals have been made to enhance the resilience to cyberthreats, elevate information protection levels within the public sector, and promote knowledge and best practices to empower citizens in safeguarding their information. This is to be achieved by improving the resilience levels of the information systems used in the public sphere and by providing the capability to effectively prevent, combat, and respond to cyberthreats. The proposed objectives can also be reached by developing competencies, knowledge and awareness of threats and challenges in the sphere of cybersecurity among public administration staff[36]. Public sector organizations often face significant challenges in securing adequate

[35] Krzysztof Kaczmarek, „Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 36.

[36] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (Warszawa: BBN, 2020), 20.

funding and resources for comprehensive cybersecurity measures, which hinders their ability to implement effective security solutions and poses a significant threat to the resilience of public services. To address these challenges, policymakers must prioritize cybersecurity funding to ensure that these organizations have the necessary tools and expertise to protect against cyberattacks and safeguard sensitive information.

The position of public institutions in cyberspace is largely determined by the information and communication technologies available to them. Due to their cost, public authorities may not always have the technologies necessary to ensure adequate protection against cyberthreats. Underfunding in the public sphere is the reason why it will not be fully protected against threats in cyberspace. It should be asserted here that information and communication technologies exposed to cyberattacks contribute to the status of public entities in the sphere of cybersecurity. We should emphasise the safe use of these technologies to avoid disruptions in providing services by electronic means. Public sector organizations often face significant challenges in securing adequate funding and resources for comprehensive cybersecurity measures. This scarcity of resources hinders their ability to implement effective security solutions and poses a significant threat to the resilience of public services. Policymakers must prioritize cybersecurity funding to ensure that these organizations have the necessary tools and expertise to protect against cyberattacks and safeguard sensitive information.

The answer to the question of whether the protection of the public sector's ICT systems is effective, being the research problem addressed in this paper, is not conclusive. On the one hand, public institutions are legally obligated to implement tools to ensure the uninterrupted operation of such systems. On the other hand, they need appropriate technical resources and software, which is not always attainable due to insufficient funding. The effectiveness of cybersecurity in the public sector hinges on a delicate balance between legal obligations, technological capabilities, and available resources. Achieving this balance ensures that security measures are both robust and practical, safeguarding critical systems and data while adhering to legal frameworks and operational constraints.

Bibliography

Casalegno Cecilia, Chiara Civera, Damiano Cortese, Alessandr Zardini, „In Search of the Enabling Factors for Public Services Resilience: A Multidisciplinary and Configurational Approach" *Journal of Innovation & Knowledge*, No. 1 (2023). https://doi.org/10.1016/j.jik.2023.100337.

Czuryk Małgorzata, „Activities of the Local Government During a State of Natural Disaster" *Studia Iuridica Lublinensia*, No. 4 (2021): 111-124. http://dx.doi.org/10.17951/sil.2021.30.4.111-124.

Czuryk Małgorzata, „Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 43-52. http://dx.doi.org/10.17951/sil.2023.32.5.43-52.

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. http://dx.doi.org/10.17951/sil.2022.31.3.31-43.

Drabik Krzysztof, „Cyberprzestrzeń – zagrożenia i wyzwania", [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. Mirosław Karpiuk. 9-20. Warszawa: ASzWoj, 2024.

Gaie Christophe, Karpiuk Mirosław, „The Provision of e-Services by Public Administration Bodies and Their Cybersecurity", [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, ed. Christophe Gaie, Mayuri Mehta. 175-188. Cham: Springer, 2024. https://doi.org/10.1007/978-3-031-55575-6_7.

Gawkowski Krzysztof, „Cyberbezpieczeństwo w inteligentnym mieście" *Cybersecurity and Law*, No. 2 (2023): 95-105. https://doi.org/10.35467/cal/174921.

Gergelewicz Tomasz, *Informacja sygnalna. Katalog obszarów działań antydezinformacyjnych.* Warszawa: ASzWoj, 2023.

Hossain Tahsin, Tan Yigitcanlar, Kien Nguyen, Yue Xu, „Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework" *Applied Sciences*, No. 13 (2024). https://doi.org/10.3390/app14135501.

Kaczmarek Krzysztof, „Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec. 29-37. Maribor: Lex Localis Press, 2022. https://doi.org/10.4335/2022.1.3.

Kaczmarek Krzysztof, „Etyka a prawo w edukacji", [in:] *Prawo w poszukiwaniu prawdy, dobra i piękna. Księga Jubileuszowa ks. prof. Sławomira Fundowicza*, ed. Paweł Śwital, Bartosz Kuś, Emilia Gulińska. 775-482. Radom: Wydawnictwo Naukowe, 2024.

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. https://doi.org/10.36128/PRIW.VI50.907.

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. https://doi.org/10.36128/priw.vi42.524.

Karpiuk Mirosław, „The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 189-201. https://doi.org/10.17951/sil.2023.32.2.189-201.

Karpiuk Mirosław, Jarosław Kostrubiec, „Provincial Governor as a Body Responsible for Combating State Security Threats" *Studia Iuridica Lublinensia*, No. 1 (2024): 107-122. https://doi.org/10.17951/sil.2024.33.1.107-122.

Karpiuk Mirosław, Claudio Melchior, Urszula Soler, „Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4 (2023): 7-27. https://doi.org/10.36128/PRIW.VI47.751.

Kellerman Aharon, *Geographic Interpretations of the Internet*, Cham: Springer, 2016.

Marczyk Maciej, „Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru" *Przegląd Teleinformatyczny*, No. 1-2 (2018): 59-72.

Miller Seumas, Terry Bossomaier, „Cybersecurity: Threats, Countermeasures, and the Institutional Landscape", [in:] *Cybersecurity, Ethics, and Collective Responsibility*, ed. Seumas Miller, Terry Bossomaier. 12-54. New York: Oxford Academic, 2024.

Mushtaq Shahrukh, Shah Mahmood, „Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management" *Information*, No. 10 (2024). https://doi.org/10.3390/info15100619.

Obermeyer Ziad, Brian Powers, Christine Vogeli, Sendhil Mullainathan, „Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations" *Science*, No. 6464 (2019): 447-453.

Sadik Shahrin Sadik, Mohiuddin Ahmed, Leslie Sikos, Najmul Islam, „Toward a Sustainable Cybersecurity Ecosystem" *Computers*, No. 9 (2020): 1-17. https://doi.org/10.3390/computers9030074.

Sandu Arun, „DevSecOps: Integrating Security into the DevOps Lifecycle for Enhanced Resilience" *Technology & Management Review*, No. 6 (2021).

Strizzolo Nicola, *Smart grid, i pericoli di una rete energetica connessa*. https://www.agendadigitale.eu/sicurezza/smart-grid-i-pericoli-di-una-rete-energetica-connessa/. [accessed: 18.11.2024].

Strizzolo Nicola, Eleonora Sparano, „Inconsapevolezza Artificiale. Dalla fiducia alla fede nelle macchine" *Sociologia. Rivista Quadrimestrale di Scienze Sociologiche, Storiche e Giuridiche*, No. 3 (2024): 6-7.

Tyrawa Dominik, „Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane" *International Journal of Legal Studies*, No 1 (2023): 13-30. https://doi.org/10.5604/01.3001.0053.9004.

Writz Berndt, Weyerer Jan, „Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats" *International Journal of Public Administration*, No. 40 (2016): 1085–1100. https://doi.org/10.1080/01900692.2016.1242614.

Zhang Mengzhong, Manpreet Kaur, „Toward a theory of e-government: Challenges and opportunities, a literature review" *Journal of Infrastructure, Policy and Development*, No. 10 (2024). https://doi.org/10.24294/jipd.v8i10.7707.

Żebrowski Andrzej, „Cyberprzestrzeń miejscem walki (wojny) informacyjnej (wybrane aspekty)", [in:] *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni*, ed. Joanna Grubicka, Aneta Kamińska-Nawrot. 9-36. Słupsk: Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, 2020.