MIROSŁAW KARPIUK, CLAUDIO MELCHIOR, URSZULA SOLER

Cybersecurity Management in the Public Service Sector

This paper refers to the issues that bring together the elements of management, law and security, which must be harmonized well enough to allow effective cybersecurity management in the public service sector, which is mainly focused on the effective performance of its tasks (also with the use of ICT systems), at local, regional and national levels. The paper aims to evaluate the processes occurring in cyberspace and the mechanisms for stimulating them, in terms of effective cybersecurity management in the public service sector. The issues related to cybersecurity management in the public service sector have not been the subject of comprehensive analyses. The subject has been treated in a fragmentary manner. Therefore, this article is part of new research. The authors have contributed equally to the study.

MIROSŁAW KARPIUK, full professor, University of Warmia and Mazury in Olsztyn
ORCID – 000-0001-7012-8999, e-mail: m_karpiuk@wp.pl
CLAUDIO MELCHIOR, associate professor, Università degli Studi di Udine
ORCID – 0000-0002-6124-4717, e-mail: claudio.melchior@uniud.it
URSZULA SOLER, associate professor, John Paul II Catholic University of Lublin
ORCID – 0000-0001-7868-8261, e-mail: urszula.soler@gmail.com

KEY WORDS: Cybersecurity, public entities, risk management, incident management

HTTPS://DOI.ORG/10.36128/PRIW.VI47.751

1 | Introduction

Since actions against cybersecurity have a significant impact on the social and public sphere, public bodies need to respond promptly and decisively to cyber-attacks, constantly searching for new state-of-the-art protection mechanisms[1]. For this purpose, the state should be able to rely on mechanisms appropriate for cybersecurity management.

In the era of the information society and the state, whose operations are largely based on information and communication systems, and where digital services are ubiquitous, cybersecurity is becoming increasingly important, as it not only facilitates uninterrupted social communication, but also enables the protection of strategic economic sectors, which makes the performance of numerous public tasks faster and more efficient[2].

The public sector is a vital factor in meeting the needs of society, both when it comes to communities at the local, regional or national level, as well as at the global level. In many countries, important public services are provided by private entities, but this paper focuses on public services. Increasingly, public authorities are using ICT systems to carry out the tasks assigned to them. Not only do they make work more efficient and effective, but they also make it possible to reduce costs and reach a wider group of people in a relatively short period of time. Since the public sector is a factor that stimulates the process of providing social services and forces the users of processes to act in a certain way, proper management in this area is of the utmost importance. Public authorities provide services and perform activities related to public powers (public administration). They shape the status of citizens within the state and influence the economy (e.g. through public procurement or the creation of favorable business conditions for certain categories of entities).

Especially in cyberspace, activities require a higher level of security in order to avoid threats that are significant for the users of ICT systems and threats that could have an impact on the normal functioning of the state and its institutions. Appropriate cybersecurity management facilitates not only the elimination of the effects of such threats, but also their anticipation

[1] Mirosław Karpiuk, „The Organisation of the National System of Cybersecurity: Selected Issues" *Studia Iuridica Lublinensia*, No. 2 (2021): 234.

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

and prevention. Given the specific nature of the digital State, information technology services, electronic communication means and the information itself, which are processed by different entities and at different scales, and which are of great importance for the functioning of the state, security in cyberspace must be duly protected in order to avoid critical disruptions.

The National Cybersecurity System Act of July 5, 201 (consolidated text, Journal of Laws of 2022, item 1863, as amended), hereinafter referred to as the NCSA, defines cybersecurity in Article 2(4) as the ability of information systems to resist actions that compromise the confidentiality, integrity, availability and authenticity of processed data or related services provided by these information systems. t is worth noting that the definition is more precise than that contained in Regulation 2019/881 of the European Parliament and of the Council (EU), according to which cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats. Pursuant to Article 4 (2) of Directive 2016/1148 of the European Parliament and the Council (EU) of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, those network and information systems. Therefore, cybersecurity not only entails counteracting and predicting threats but also eliminating the outcomes of their occurrence. Cyberspace is the domain in which such threats and their effects occur[3]. It is defined in Article 2(1a) of the State of Emergency Act of 21 June 2002 (consolidated text, Journal of Laws of 2017, Item 1928) as a space for the processing and exchange of information created by ICT systems, including the links between them and their relations with users.

Cybersecurity management involves harmonizing the processes that take place in cyberspace to protect against the threats that occur there. Therefore, its goal is to coordinate the protection mechanisms that allow the mitigation of cyber threats, thus ensuring the continuity and effectiveness of ICT systems at the lowest possible cost. Designing cyber processes that affect the delivery of electronic services not only increases the efficiency

[3] Mirosław Karpiuk, „The Local Government's Position in the Polish Cybersecurity System" *Lex Localis. Journal of Local Self-Government*, No. 3 (2021): 612.

of ICT systems, but also improves their protection against disruptions and cyber attacks. However, those responsible for risk assessment face numerous challenges related to innovative cyber systems. These challenges include the constantly evolving nature of cybernetic systems based on technological progress, their distribution across physical, information and socio-cognitive domains, and complex network structures that often involve thousands of nodes[4].

Cybersecurity management can be divided into the following stages: detection, assessment, remediation and recommendations. Detection of a threat triggers the cybersecurity management process. Without detection, remediation is not possible. The assessment of threats and potential consequences that occur in cyberspace is aimed at defining their status and classifying them. It facilitates the use of appropriate cybersecurity management tools (appropriate for a given threat) to immediately initiate remedial actions. Remedial action is a stage in which given cyber threats are eliminated (if the cost of such action is not disproportionate to the objective to be achieved by it) and their results are removed (if there were any). At the recommendation stage, it is necessary to determine what actions should be taken to prevent incidents of a particular type from occurring in the future. This includes the development of recommendations that should be considered in the course of securing a given ICT system against disruptions.

2 | Literature review

The issue of cybersecurity is being analyzed in an increasingly extensive manner in Polish and foreign literature on the subject. It is treated as a matter of common interest[5]. Security in cyberspace is a crucial element enabling the efficient performance of public tasks using ICT systems, which must be properly protected against cyber attacks, which in certain

[4] Alexander Ganin, Phuoc Quach, Mahesh Panwar, Zachary Collier, Jeffrey Keisler, Dayton Marchese, Igor Linkov, „Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management" *Risk Analysis*, No. 1 (2020).

[5] Jarosław Kostrubiec, „The position of the Computer Security Incidents Response Teams in the national cybersecurity system" *Cybersecurity and Law*, No. 2 (2022): 34.

cases may even paralyze the operations of a given authority[6]. M. Czuryk also discusses the issues of cybersecurity, noting that it is a specialized component of the security system, which includes the protection of information systems against threats[7]. It is right to agree with the view that cybersecurity is one of the types of security[8]. It is worth mentioning here that security not only allows to fulfill social needs, but also ensures uninterrupted functioning of public institutions[9], and threat prevention is one of its most important stages[10]. It is precisely prevention (of cyberattacks) that is one of the objectives of cybersecurity management. What is significant is that cybersecurity management is conducted in many different areas, for instance, in logistics, which is comprehensively discussed by the authors of a paper entitled *Cybersecurity in logistics and supply chain management: An overview and future research directions*[11], in internet voting processes[12] or the local government sector[13]. In their article entitled *Cyber Security Management: A Review,* Kouroush Jenab and Saeid Moslehpour[14] provide a summary of cybersecurity management issues and assert that cybersecurity, which involves the protection of both data and people, faces

[6] Istvan Hoffman, Mirosław Karpiuk, „E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues" *Lex Localis. Journal of Local Self-Government*, No. 3 (2022): 628.

[7] Małgorzata Czuryk, „Supporting the Development of Telecommunications Services and Networks Through Local and regional Government Bodies and Cybersecurity" *Cybersecurity and Law*, No. 2 (2019): 42.

[8] Dominik Tyrawa, „The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 23.

[9] Mirosław Karpiuk, „The Provision of Safety in Water Areas: Legal Issues" *Studia Iuridica Lublinensia*, No. 1 (2022): 82.

[10] Małgorzata Czuryk, „Activities of the Local Government During a State of Natural Disaster" *Studia Iuridica Lublinensia*, No. 4 (2021): 122.

[11] Cheung Kam-Fung, Bell Michael, Bhattacharjya Jyoti, „Cybersecurity in Logistics and Supply Chain Management: An Overview and future Research Directions" *Transportation Research Part E: Logistics and Transportation Review*, No. 146 (2021).

[12] Tadas Limba, Tomas Plėta, Konstantin Agafonov, Martynas Damkus, "Cyber Security Management Model for Critical Infrastructure" *Entrepreneurship and Sustainability Issues*, No. 4 (2017).

[13] Aneta Chodakowska, Sławomira Kańduła, Joanna Przybylska, „Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done" *Lex Localis. Journal of Local Self-Government*, No. 1 (2022).

[14] Kouroush Jenab, Saeid Moslehpour, „Cyber Security Management A Review" *Business Management Dynamics*, No.11 (2016).

multiple threats, particularly cybercrime and online industrial espionage, both of which are growing rapidly.

According to K. Chałubińska-Jentkiewicz, activities in virtual space are characterized by a specific culture of user behavior within the virtual community. Therefore, it should be assumed that cybersecurity creates a need to consider situations that do not necessarily need to have their counterpart in the world outside cyberspace. The notion of cybersecurity may refer to the spheres related to information security, communication security or the security of a particular ICT system itself[15]. It is noted in the literature on the subject that the possibilities offered by digital technologies are also used for adverse activities, including unfair competition practices, disrupted provision of digital services, offences committed with the use of the Internet, or terrorist operations[16]. ICT systems may have various applications, and some of them can also be used for illegal activities. Effective cybersecurity management is aimed at eliminating adverse actions – those affecting the public and economic spheres, and those which compromise the sphere of human rights and civil liberties.

ICT systems are not only useful for finding information, but also for conducting business activities, providing various types of services, communicating, and performing public functions. Their importance to the public sector or the economy may be a priority issue. Therefore, they must be properly protected, sometimes at the expense of human freedoms and rights[17]. Due to the need to ensure the cybersecurity of the State, special emphasis should be placed on countering incidents that have or could have a negative impact on the functioning of information systems, in particular critical incidents[18].

W. Pizło deals with the issues which directly concern management in cyberspace, indicating the need to apply the resulting principle of zero trust to any users or any processes, which constitutes a new paradigm of

[15] Chałubińska-Jentkiewicz Katarzyna, „Cyberbezpieczeństwo – zagadnienia definicyjne" *Cybersecurity and Law*, No. 2 (2019): 13.

[16] Jarosław Kostrubiec, „Cybersecurity System in Poland. Selected Legal Issues", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 8.

[17] Małgorzata Czuryk, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 40.

[18] Mirosław Karpiuk, „The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights" *Przegląd Prawa Konstytucyjnego*, No. 3 (2022): 407.

cybersecurity, according to which it is assumed that users should have a minimum network access that allows the successful performance of the entrusted activities[19]. Due to the threats that exist in cyberspace and its use not only for peaceful purposes, raising the awareness of users and equipping them with the skills that allow them to develop their competencies based on knowledge of the nature and functioning of cyberspace is one of the most important tasks in the field of cyber security[20].

It should be emphasized that the issue of cybersecurity management in many situations can be traced back to the fact that cybersecurity is still usually treated as a technical aspect or technology that can be easily implemented in an organization. And such implementation guarantees cybersecurity. As the authors quoted above point out, cybersecurity today is more than just technology; it also includes cultural, legal, and psychological aspects. In order to create an effective cybersecurity management system, especially in the critical infrastructure sector, cybersecurity management models are designed and can be used to ensure the security of critical infrastructure in an organization or company[21].

It is worth noting that systems thinking, self-organizing teams, individual and team innovation and creativity, and delegation of authority and responsibility are the foundation of modern management[22]. They also refer to cybersecurity management in the public service sector as well.

[19] Wojciech Pizło, „Management in Cyberspace: From Firewall to Zero Trust", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 144.

[20] Anna Makuch, „Raising Public and Private User Awareness of the Threats and Risks Related to Cyberspace Security" *Cybersecurity and Law*, No. 2 (2022): 53.

[21] Elżbieta Szczepankiewicz, „Model zarządzania bezpieczeństwem informacji korporacyjnych w przedsiębiorstwie" *Przedsiębiorczość i Zarządzanie*, No. 2 (2018); Tadas Limba, Tomas Plėta, Konstantin Agafonov, Martynas Damkus, „Cyber Security Management Model for Critical Infrastructure" *Entrepreneurship and Sustainability Issues*, No. 4 (2017); Lech Kościelecki, Karolina Doran, „Model zarządzania bezpieczeństwem informacji w przedsiębiorstwie" *Systemy Logistyczne Wojsk*, No. 4 (2017).

[22] Barbara Wyrzykowska, Tetiana Balanowska, „Zarządzanie w warunkach rewolucji cyfrowej", [in:] *Współczesne obszary zarządzania*, ed. Wojciech Pizło (Warsaw: SGGW, 2021), 25.

3 | Methodology

The objective of the paper is to identify the mechanisms that allow an effective cybersecurity management in the public service sector, aimed on the one hand at the proper management of public funds and on the other hand at the protection of the ICT systems of public entities against cyber threats and at the investment in protection.

The main research problem can be expressed by posing the following question:

- (RP1) – Does cybersecurity management contribute to better protection of ICT systems used by public entities to perform the tasks they have been entrusted with without the need to limit the availability of the systems?

In addition, three specific research questions can be formulated as follows:

- (RP2) – Do cybersecurity management mechanisms allow for network security?
- (RP3) – Does cybersecurity management enable public entities to optimise occurring costs on their operations in cyberspace?
- (RP4) – What actions should be taken in the public service sector to ensure secure electronic service delivery?

With regard to the hypothesis formulated, it should be assumed that (H1) efficient management in the public service sector contributes to improving the security of ICT systems. This mainly refers to cybersecurity management (as a part of organizational management), which should prevent disruptions in the operation of systems and allow for the prompt elimination of their consequences, thus facilitating the continuity of public service provision.

The main research method applied in the paper is the doctrinal legal research method[23]. It was used to analyze the applicable legal regulations governing the issues of cybersecurity provision in the public service sector

[23] Janusz Guść, „Dogmatyka prawa", [in:] *Leksykon współczesnej teorii i filozofii prawa. 100 podstawowych pojęć*, ed. Jerzy Zajadło (Warsaw: C.H. Beck, 2007), 53–54.

and the issues related to management in cyberspace, including, in particular, risk or incident management. The method was also used to analyze the normative solutions adopted by the legislator, while the evaluation mainly concerned the regulations directly applicable to the management of cybersecurity in the public sphere. The legal-theoretical method was also used[24], with the aim of evaluating the activities of public authorities in cyberspace in terms of their obligations to ensure the safe use of ICT systems, both by the entities that perform their public tasks through such systems and by the beneficiaries of these activities.

The authors also used the quantitative statistical method to study the occurrence of incidents in the period covered by the study, in general, and incidents involving public entities, particularly those recorded for the public administration sector.

4 | Results

Cybersecurity management is related to the proper handling of incidents, defined in Article 2 (10) of the NCSA as activities that allow not only the detection, recording, analysis and classification of incidents but also remedial measures and mitigation of incident outcomes. As regards cybersecurity management in the public sector, this refers to incident handling in public entities. Under Article 2 (9) of the NCSA, an incident in a public entity means an incident which results, or might result, in the deterioration of quality or the disruption of public tasks performed by a public entity. It is consistent with the definition of "incident" in European law (Directive (EU) 2022/2555 of the European Parliament and of the Council) according to which it means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or of the services offered by, or accessible via, network and information systems.

The analysis includes incidents that took place between 2019 and 2022, which is related to the fact that 2019 was the first year in which the NCSA was in force, which means that the activities related to cybersecurity management and countering cyberattacks were regulated by law, which

[24] Ryszard Sarkowicz, Jezry Stelmach, *Teoria prawa* (Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, 2001).

significantly facilitated the elimination of negative phenomena in cyberspace. The end date is 2022.

The analysis covers incidents reported to CSIRT NASK (Computer Security Incident Response Team operating at the national level and managed by the Research and Academic Computer Network – National Research Institute). Due to the restricted access to information about incidents handled by CSIRT GOV (Computer Security Incident Response Team operating at the national level and managed by the Head of the Internal Security Agency) and CSIRT MON (Computer Security Incident Response Team operating at the national level and managed by the Minister of National Defence), which are related to state security, the analysis does not cover such incidents.

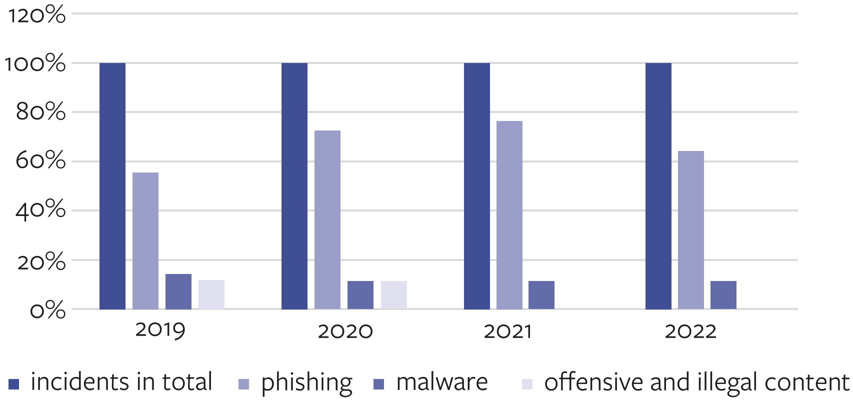
In 2019, 6484 incidents were recorded in Poland. Phishing was the most frequently occurring attack, accounting for 54.2% of all incidents. Incidents related to malware came in second place, with a share of 14.9%. Incidents described as offensive and illegal content accounted for 12.1% of all recorded incidents in 2019[25]. In turn, 10,420 incidents were recorded in 2020. Similar to the preceding year, the most popular type of incident was phishing which comprised 73% of all handled incidents. Malware was the second most common type of incident, accounting for 7.16% of all incidents. It was followed by incidents belonging to the offensive and illegal content category. They accounted for 3.22% of all incidents[26]. 2021 saw the most significant increase in the number of recorded incidents in a period under analysis. A total of 29,483 incidents were recorded that year. Similar to preceding years, phishing was the most frequent type of incident. It accounted for 76.57% of the total number of incidents. The second type of recorded incidents was malware, with a share of 9.66% of all incidents. The third position was taken by offensive and illegal content, accounting for 1.05%[27]. As per the 2022 data obtained from CSIRT NASK, 39,683 incidents were recorded that year, with phishing having a share of 64.57%, malware constituting 8.59% of all incidents, and offensive and illegal content accounting for 0.77% of all incidents.

[25] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska* (Warsaw: NASK.CERT.PL, 2020), 9.

[26] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2020 z działalności CERT Polska* (Warsaw: NASK.CERT.PL, 2021), 25.

[27] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2021 z działalności CERT Polska* (Warsaw: NASK.CERT.PL, 2022), 20.

Fig. 1. The most frequent incidents registered by the CSIRT NASK in 2019–2022



Source: The author, based on annual reports for 2019–2022 regarding the activities of CERT Poland

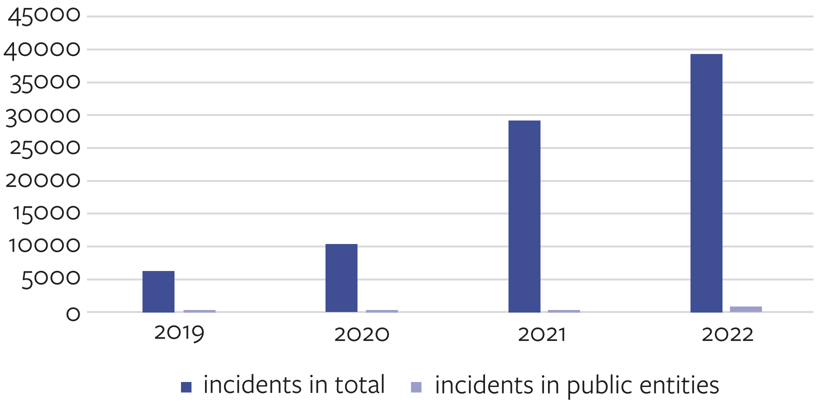
In 2019, the CSIRT NASK recorded 336 incidents affecting public institutions, which accounted for 5.2% of all recorded incidents. Reports from this sector were most often classified as malware or offensive and illegal content. There were also phishing attacks aimed at obtaining email authentication credentials[28]. On the other hand, in 2020, the NASK CSIRT handled 461 incidents concerning public institutions, which represents 4.4% of all recorded incidents. Notifications from the sector most frequently concern malware or offensive and illegal content. Phishing attacks occurred as well, targeting e-mail authentication data, similarly to the preceding year[29]. In 2021, CSIRT NASK recorded another increase in the number of incidents affecting public entities, with 512 such incidents accounting for 1.74% of the total incident number[30]. Based on the information provided by CSIRT NASK, in 2022 there were 937 incidents affecting public entities and they accounted for 2.36% of all incidents.

[28] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska* (Warsaw: NASK.CERT.PL, 2020), 14.

[29] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2020 z działalności CERT Polska* (Warsaw: NASK.CERT.PL, 2021), 25.

[30] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2021 z działalności CERT Polska* (Warsaw: NASK.CERT.PL, 2022), 21.

Fig. 2. Incidents concerning public entities registered by CSIRT NASK in 2019–2022

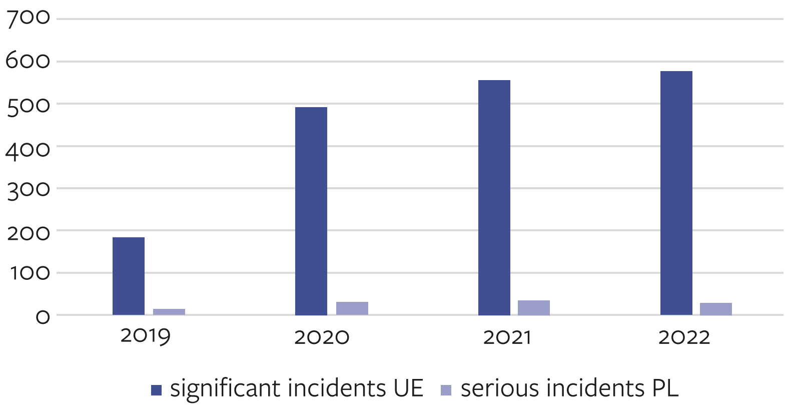


Source: The author, based on annual reports for 2019–2022 regarding the activities of CERT Poland

There is a significant increase in the number of incidents from year to year. In 2021, there were more than twice as many incidents as in the previous year, and in 2019, there were 4.5 times as many incidents. There was also a further increase in 2022. The upward trend also applies to incidents in public institutions, although their number did not increase as dramatically as the total number of incidents.

At the European Union level, the statistical data collected by the European Union Agency for Cybersecurity (ENISA) includes cybersecurity incidents which pose a significant threat. The Polish legislator does not distinguish between such incidents and refers to serious incidents. The data on significant incidents is collected by ENISA, which not only anonymizes and aggregates the data, but also analyzes it.

Fig. 3. Significant incidents recorded by ENISA and serious incident by CSIRT NASK in the years 2019–2022



Source: The author, based on annual reports for 2019–2022 regarding the activities of CERT Poland and based on ENISA data available on https: https://ciras.enisa.europa.eu/ciras-consolidated-reporting [accessed: 9.03.2023]

According to statistical data on significant incidents reported with ENISA, there were 185 such incidents in 2019, and 495 in 2020, while in 2021, ENISA recorded 559 such incidents, and the following year, 2022, saw a further increase, as there were 580 significant incidents during that period[31].

According to CSIRT NASK, the quantitative structure of significant incidents between 2019 and 2022 was as follows: 2019 – 14, 2020 – 32, and 2021 – 36, with 30 serious incidents reported in 2022.

5 | Discussion

Risk management is one of the elements of cybersecurity management because ICT systems, including those used by the public sector, are constantly exposed to cyber-attacks and the risk of such attacks is significant. Risk management is defined in Article 2 (19) of the NCSA as coordinated actions in the area of cybersecurity management regarding the estimated

[31] Incident reporting. https://ciras.enisa.europa.eu/ciras-consolidated-reporting. [accessed: 9.03.2023].

risk, understood as the probability of occurrence of an adverse event and its consequences.

With respect to organizations that conduct their activities in cyberspace, risk management includes the following elements: 1) identifying objectives, 2) specifying risks, 3) assessing the likelihood of an adverse event occurring, 4) preventing and mitigating the effects of a cyber attack, and 5) monitoring threats. The above cyber risk management components are minimized depending on the skills of the IT security staff and the level of cooperation with other structures within a given organization[32].

Another element of cybersecurity management is the management of incidents, a phenomenon that has or could have a negative impact on cybersecurity. According to Article 2 (18) of the NCSA, incident management is understood as the handling of incidents, the identification of links between incidents, the elimination of the cause of incidents and the development of conclusions arising from the handling of incidents.

Cybersecurity management in the public sector refers to public entities that make up the national cybersecurity system, including selected entities in the public finance sector and Computer Security Incident Response Teams (CSIRT). The objective of the system, and therefore of the policies developed by the entities that form it, as defined in Article 3 of the NCSA, is to ensure cybersecurity, which includes the uninterrupted provision of essential services and digital services, by achieving the appropriate level of security of the information systems used to provide these services and by ensuring incident handling operations.

Cybersecurity management is directly related to ensuring the security of services provided by electronic means, including the services offered by public entities. In line with the definition set out in Article 2(4) of the Act of July 18, 2002 on the Provision of Services by Electronic Means (consolidated text, Journal of Laws of 2020, item 344, as amended), the provision of services by electronic means is defined as the provision of a service without a simultaneous presence of the parties (remotely), through the transfer of data at the customer's request, transmitted and received with the use of electronic data processing devices, and fully sent, received and transmitted via an ICT network. A public entity acting as a service provider is obliged to ensure the uninterrupted operation of an ICT system that

[32] Wojciech Pizło, „Management in Cyberspace: From Firewall to Zero Trust", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 137.

provides a given service. This includes preventing unauthorized access by third parties.

Cybersecurity management falls within the sphere of crisis management, especially if this pertains to the owners, owner-like possessors or lessees of facilities, installations, and devices which comprise critical infrastructure, who are at the same time operators of essential services. It should be stressed here that the sphere of crisis management is affected by legislative chaos. It involves the fact that statutory regulations are based on ostentatious solutions (of minor normative significance), which specify a comprehensive list of tasks entrusted to public authorities without providing any resources to allow their performance. Moreover, the responsibilities and forms of actions of these authorities are specified in various planning documents, although these issues should be regulated in generally applicable normative acts[33]. Cyber threats might give rise to various adverse phenomena, including crises, especially if cyber-attacks are directed against ICT systems used by public entities to perform public tasks of strategic importance, including those related to the continued operation of critical infrastructure. Threats in cyberspace could lead to crises, as public institutions are largely digitized and the ICT systems they use do not always meet adequate security standards[34].

Disruptions in cyberspace might have a negative effect on the functioning of the state, which is to ensure the appropriate quality of the services it provides, including services of strategic importance. Due to the need to properly secure such services, including their continuity and suitable reach (availability), it is necessary to undertake administrative measures to protect them in full[35]. In view of the above, it should be emphasized that proper cybersecurity management facilitates the development of recommendations within the framework of the correct standards of rendering services by electronic means, including their security should be provided.

[33] Mirosław Karpiuk, Tomasz Włodek, „Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)” *Studia Iuridica Lublinensia*, No. 1 (2020): 274.

[34] Mirosław Karpiuk, „Crisis Management vs Cyber Threats” *Sicurezza, Terrorismo e Societa*, No. 2 (2022): 114.

[35] Idem, „Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level” *Prawo i Więź*, No. 4 (2022): 167–168.

6 | Conclusions

In recent years, the management of cyberspace has been dominated by people who professionally deal with the construction of ICT systems and networks. These circles have imposed their image of cyberspace, limiting their activities mainly to technological issues. A management-oriented approach to cybersecurity refers to the social dimension of the relationships between individual employees and between employees and their devices. The pervasiveness of information technologies affects the shape of organizations, which is related to the universal flow of information. The structures of many organizations are being simplified and government is being digitized. The rapid development of cyberspace is contributing to changes in social relations, while management methods are being modified to adapt to the changing reality. Cyber management, whose goal is to manage the resources available to an organization, is a vital area of cyberspace. The scope of management activities is defined, on the one hand, by national and international laws and, on the other hand, by the individual skills of managing digital resources in an organization[36].

In principle, new technologies should always serve the interests of society, its individual members or social groups, but there is no guarantee that they will always be used as intended due to the lack of restrictions and easy availability. The misuse of new technologies can jeopardize cybersecurity (including cybersecurity in the public sector), so the public administration must invest in solutions that are characteristic of modern management in cyberspace, which is not only to support the optimization of the administration's task performance, but also to build a security system that is adequate to the threats and allows the uninterrupted operation of ICT systems used for the performance of public tasks.

The nature of the Internet favors a reduced sense of responsibility. Relatively cheap access to data resources makes it a tool for making work, learning and entertainment easier. Relatively cheap access to data resources makes it a tool for facilitating work, learning and entertainment. In the area of information exchange infrastructure, it serves to liberalize professional life. In the social, commercial, and political spheres, it offers

[36] Wojciech Pizło, „Management in Cyberspace: From Firewall to Zero Trust", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 143–144.

not only free participation and convenient data management solutions, but also a wide range of opportunities to manipulate information, preferences, and attitudes[37]. Such manipulations are a cybersecurity threat and may be eliminated in the event of proper management of the sphere, based on the application of new technologies, or using Artificial Intelligence, as well as based on investments in human potential – in good managers.

Cybersecurity management must take into account the principle of minimizing disruptions to the operation of ICT systems, which is a rule that also refers to limiting their availability to users. It should facilitate faster detection of defects in ICT systems, including possible weaknesses in their security, and prevent irreversible destruction of data processed in the systems. One of the objectives of management is to identify the vulnerabilities of a given ICT system that affect its integrity, confidentiality or availability. These vulnerabilities can be used to launch cyber attacks.

Cybersecurity management must lead to the formulation of conclusions and guidelines that would prevent further threats by detecting them earlier and minimizing their impact after a given threat has already occurred.

Due to limited public funds and the need to allocate them rationally, resource management is becoming increasingly important. Optimized spending is also facilitated by the use of cyberspace to address specific societal needs. In addition, cyberspace must be properly secured and resilient to significant threats. It is the management of cybersecurity that favors the balance of spending on cyberspace protection in the performance of public tasks with the use of ICT systems and the limited financial resources at the disposal of public entities.

The answer to the research question of whether cybersecurity management contributes to better protection of ICT systems used by public sector entities to perform the tasks entrusted to them, without the need to limit the availability of the systems, should be in the affirmative. Cybersecurity management favors such protection, although it is not always possible to restore the operation of a given ICT system without limiting its availability, in particular when repair activities are carried out.

When addressing the underlying research problem stated in the article, it should be noted that cybersecurity management fosters better protection

[37] Anna Makuch, „Strategic and Political Responsibility in the Domain of Cybersecurity – Problems and Challenges", [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, ed. Katarzyna Chałubińska-Jentkiewicz, Istvan Hoffman (Maribor: Lex Localis Press, 2022), 75.

of ICT systems used by public entities to implement the tasks assigned to them and facilitates their implementation process. The questions that constitute specific research problems cannot always be answered affirmatively. First, the mechanisms specific to cybersecurity management do not ultimately guarantee network security. Second, cybersecurity management optimizes costs incurred by public entities in connection with their cyberspace operations, provided that it is approached professionally and continuously. Third, to ensure the security of electronic service delivery in the public service sector, one should rely on staff with the appropriate knowledge and skills, and on investments in software and hardware to ensure cybersecurity.

Attention should be paid to the legal solutions binding in the European Union that are relevant for cybersecurity. Directive 2022/2555 of the European Parliament and of the Council of December 14, 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, determines measures aimed at a high common level of cybersecurity across the Union, to improve the functioning of the internal market. Account should also be taken of Regulation 2022/2554 of the European Parliament and of the Council of December 14, 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) No 2016/1011, adopted to attain a high common level of digital operational resilience through laying down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities, which is also crucial for public services.

Finally, it should be emphasized that public tasks are carried out by administrations (i.e. state and local administrations) at the central, local and regional levels. This results from the need to adapt both the tasks and their scope not only to the form of public administration prevailing in the country, but also to the actual needs, quality and availability of the services provided, as well as to optimize the costs of their provision[38].

[38] Mirosław Karpiuk, „Position of the Local Government of Commune Level in the Space of Security and Public Order” *Studia Iuridica Lublinensia*, No. 2 (2019): 27–28.

Bibliography

Chałubińska-Jentkiewicz Katarzyna, „Cyberbezpieczeństwo – zagadnienia definicyjne” *Cybersecurity and Law*, No. 2 (2019): 7–23. doi.org/10.35467/cal/133828.

Cheung Kam-Fung, Bell Michael, Bhattacharjya Jyoti, „Cybersecurity in Logistics and Supply Chain Management: An Overview and Future Research Directions” *Transportation Research Part E: Logistics and Transportation Review*, No. 146 (2021): 1–18. https://doi.org/10.1016/j.tre.2020.102217.

Chodakowska Aneta, Sławomira Kańduła, Joanna Przybylska, „Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done” *Lex Localis. Journal of Local Self-Government*, No. 1 (2022): 161–192. doi.org/10.4335/20.1.161-192(2022).

Czuryk Małgorzata, „Supporting the Development of Telecommunications Services and Networks Through Local and Regional Government Bodies and Cybersecurity” *Cybersecurity and Law*, No. 2 (2019): 39–50. doi.org/10.35467/cal/133839.

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

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. doi.org/10.17951/sil.2022.31.3.31-43.

Ganin Alexander, Phuoc Quach, Mahesh Panwar, Zachary Collier, Jeffrey Keisler, Dayton Marchese, Igor Linkov, „Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management” *Risk Analysis*, No. 1 (2020): 183–199. doi.org/10.1111/risa.12891.

Guść Janusz, „Dogmatyka prawa”, [in:] *Leksykon współczesnej teorii i filozofii prawa. 100 podstawowych pojęć*, ed. Jerzy Zajadło. 53–54. Warsaw: C.H. Beck, 2007.

Hoffman Istvan, Mirosław Karpiuk, „E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues” *Lex Localis. Journal of Local Self-Government*, No. 3 (2022): 617–640. doi.org/10.4335/20.3.617-640(2022).

Incident reporting. https://ciras.enisa.europa.eu/ciras-consolidated-reporting.

Jenab Kouroush, Saeid Moslehpour, „Cyber Security Management A Review” *Business Management Dynamics*, No. 11 (2016): 6–39.

Karpiuk Mirosław, „The Organisation of the National System of Cybersecurity: Selected Issues” *Studia Iuridica Lublinensia,* No. 2 (2021): 233–244. doi.org/10.17951/sil.2021.30.2.233-244.

Karpiuk Mirosław, „The Local Government's Position in the Polish Cybersecurity System" *Lex Localis. Journal of Local Self-Government*, No. 3 (2021): 609–620. doi.org/10.4335/19.3.609-620(2021).

Karpiuk Mirosław, „Crisis Management vs Cyber Threats" *Sicurezza, Terrorismo e Societa*, No. 2 (2022): 113–123.

Karpiuk Mirosław, „Position of the Local Government of Commune Level in the Space of Security and Public Order" *Studia Iuridica Lublinensia*, No. 2 (2019): 27–39. doi.org/10.17951/sil.2019.28.2.27-39.

Karpiuk Mirosław, „Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź*, No. 4 (2022b): 166–179. 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. doi.org/10.17951/sil.2023.32.2.189-201.

Karpiuk Mirosław, „The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights" *Przegląd Prawa Konstytucyjnego*, No. 3 (2022c): 401–412. doi.org/0.15804/ppk.2022.03.30.

Karpiuk Mirosław, „The Provision of Safety in Water Areas: Legal Issues" *Studia Iuridica Lublinensia*, No. 1 (2022): 79–92. doi.org/10.17951/sil.2022.31.1.79-92.

Karpiuk Mirosław, Tomasz Włodek, „Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)" *Studia Iuridica Lublinensia*, No. 1 (2020): 273–290. doi.org/10.17951/sil.2020.29.1.273-290.

Kostrubiec Jarosław, „Cybersecurity System in Poland. Selected Legal Issues", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec. 7–17. Maribor: Lex Localis Press, 2022. doi.org/10.4335/2022.1.1.

Kostrubiec Jarosław, „The Position of the Computer Security Incidents Response Teams in the National Cybersecurity System" *Cybersecurity and Law*, No. 2 (2022): 27–37. doi.org/10.35467/cal/157121.

Kościelecki Lech, Karolina Doran, „Model zarządzania bezpieczeństwem informacji w przedsiębiorstwie" *Systemy Logistyczne Wojsk*, No. 4 (2017): 107–134.

Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska. Warsaw: NASK.CERT.PL, 2020.

Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2020 z działalności CERT Polska. Warsaw: NASK.CERT.PL, 2021.

Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2021 z działalności CERT Polska. Warsaw: NASK.CERT.PL, 2022.

Limba Tadas, Tomas Plėta, Konstantin Agafonov, Martynas Damkus, „Cyber Security Management Model for Critical Infrastructure” *Entrepreneurship and Sustainability Issues*, No. 4 (2017): 559–573. http://dx.doi.org/10.9770/jesi.2017.4.4(12).

Makuch Anna, „Strategic and Political Responsibility in the Domain of Cybersecurity – Problems and Challenges”, [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, ed. Katarzyna Chałubińska-Jentkiewicz, Istvan Hoffman. 69–78. Maribor: Lex Localis Press, 2022. doi.org/10.4335/2022.2.5.

Makuch Anna, „Raising Public and Private User Awareness of the Threats and Risks Related to Cyberspace Security” *Cybersecurity and Law*, No. 2 (2022): 44–55. doi.org/10.35467/cal/157123.

Pizło Wojciech, „Management in Cyberspace: From Firewall to Zero Trust”, [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec. 133–146. Maribor: Lex Localis Press, 2022. doi.org/10.4335/2022.1.13.

Sarkowicz Ryszard, Stelmach Jerzy, *Teoria prawa*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, 2001.

Soler Urszula, „The Role of Network Technologies in European Cybersecurity”, [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. Katarzyna Chałubińska-Jentkiewicz, Istvan Hoffman. 47–58. Maribor: Lex Localis Press, 2022. doi.org/10.4335/2022.2.3.

Szczepankiewicz Elżbieta, „Model zarządzania bezpieczeństwem informacji korporacyjnych w przedsiębiorstwie” *Przedsiębiorczość i Zarządzanie*, No. 2 (2018): 191–209.

Tyrawa Dominik, „The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity”, [in:] *The Public Dimension of Cybersecurity*, eds. Mirosław Karpiuk, Jarosław Kostrubiec. 19–37. Maribor: Lex Localis Press, 2022. doi.org/10.4335/2022.1.2.

Wyrzykowska Barbara, Tetiana Balanowska, „Zarządzanie w warunkach rewolucji cyfrowej”, [in:] *Współczesne obszary zarządzania*, ed. Wojciech Pizło. 13–28. Warsaw: SGGW, 2021.

Zeliaś Aleksander, *Metody Statystyczne*. Warsaw: Polskie Wydawnictwo Ekonomiczne, 2000.