Ewa Maria Włodyka[*]
Krzysztof Kaczmarek[**]

Cyber Security of Electrical Grids – A Contribution to Research

Abstract

The state's critical infrastructure involves those elements that function independently yet are interconnected. It is also affected by ICT networks that exist in other states. These interdependencies make critical infrastructure particularly vulnerable to cyber attacks. At the same time, it is electrical grids that constitute the most crucial element of critical infrastructure. The research hypothesis assumes an urgent need to comprehensively address the cyber security policy of electrical grids in a broader perspective, not only the technical one but also taking into account public policies and the human factor. Quantitative and qualitative methods, literature survey and the desk research method were employed in order to verify this hypothesis.

The analyses carried out by the Authors indicated unequivocally that electrical grids constitute an element of the critical infrastructure that is the most vulnerable to cyber threats.

Key words: electrical grids, public administration, cyber security, critical infrastructure

[*] Ewa Maria Włodyka, PhD, Faculty of Humanities, Koszalin University of Technology, e-mail: ewa.wlodyka@tu.koszalin.pl; ORCID: 0000-0002-8229-342X.

[**] Krzysztof Kaczmarek, PhD, Faculty of Humanities, Koszalin University of Technology, e-mail: puola@tlen.pl; ORCID: 0000-0001-8519-1667.

Introduction

The proper functioning of modern societies, states and supranational structures is largely based on access to information[1]. At the same time, this access is made possible by properly functioning telecommunications networks. These in turn operate based on electricity. Stable electricity supply depends both on its correct distribution and primary energy sources. Without it, the Internet does not function – and it is already so ubiquitous that it forms part of numerous items: the Internet of Things (IoT). Electric grid cybersecurity risk has become a significant concern for industries and governments[2]. Hence, cyber-security of electrical grids is related both to private and public sectors. Russia's military aggression against Ukraine, which began on 24 February 2022, had repercussions that changed the global balance of power and the geopolitics of many countries, and it caused turbulence in the energy market and, above all, in the hydrocarbons market[3]. As a result, the energy security of countries whose economies rely on fossil fuels decreased. This situation demonstrated that the proper functioning of digital societies is exposed to a number of threats. On the one hand, these are disruptions to the stable functioning of network services and, on the other, they result from the malfunctioning of these services. The functioning of the entire Internet is based on the consumption of electricity. In turn, the control of electricity distribution is based on ICT links. At the same time, all network services are vulnerable to disruptions, especially those caused by cyber attacks. Successful cyber attacks, on the other hand, may cause, among other things, interruptions in the supply of electricity, resulting in the shutdown of further network services. In such a case, a chain reaction with consequences that are difficult to predict may be initiated. Cyber disruptions can adversely affect the quality of critical services and the proper functioning of society and the state[4].

[1] M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2, p. 646.

[2] X. Diao et. al., *Dynamic probabilistic risk assessment for electric grid cybersecurity*, „Reliability Engineering & System Safety" 2024, no. 109699.

[3] K. Kaczmarek, E. Włodyka, *Strategiczne znaczenie Cieśniny Ormuz i jego implikacje dla bezpieczeństwa energetycznego Europy w kontekście agresji Rosji na Ukrainę*, „Studia Gdańskie. Wizje i Rzeczywistość" 2022, vol. 19, p. 209–210.

[4] M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2, p. 198.

Security is an area of particular concern for the state, which has a duty to ensure freedom from or neutralisation of threats that disrupt the normal functioning of public institutions, private entities and society[5]. This also applies to the area of cyber security, of which the local government is one of the actors[6]. At this point, it should be noted that in philosophical terms, security means the certainty of survival, elimination of threats and possibility of development in accordance with one's own principles[7].

The aim of this article is to make a contribution to research on comprehensive understanding of the cyber security of electrical grids in a broader perspective.

The research hypothesis points to an urgent need for comprehensive understanding of the electrical grid cyber security policy in a broader perspective, not only a technical one but also taking into account public policies and the human factor.

The following methods will be employed to verify this hypothesis: qualitative, literature survey, comparative and desk research methods.

Security in cyberspace

There are many methods and targets for cyber attacks, but those targeting telecommunications networks have the potential to disrupt the proper functioning of all the elements of critical infrastructure[8]. It should also be emphasized that the nature of cyber threats, like cyber defences, is dynamic, and actions in cyberspace may lead to armed conflict[9]. However, responsible and unprovocative behaviour by Internet users does not appear to be standard. This is because cyberspace is a completely new environment for humanity. Thus, there is no tradition of passing on knowledge from one generation to

[5] Idem, *Organisation of the National System of Cybersecurity: Selected Issues*, ibidem 2021, no. 2, p. 234.

[6] J. Kostrubiec, *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland*, „Lex Localis – Journal of Local Self-Government" 2021, no, 1, p. 115.

[7] M. Karpiuk, A. Makuch, U. Soler, *The Role of the Cybersecurity Strategy of the Republic of Poland in Ensuring Cybersecurity*, „Polish Political Science Yearbook" 2023, no. 3, p. 63.

[8] M. Karpiuk, *Crisis management vs. cyber threat*, „Sicurezza, Terrorismo e Società" 2022, no. 2, p. 114.

[9] A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2, p. 28.

the next and, bringing with it a new, post-modern quality of life, cyberspace generates certain problems and risks, the number of which is increasing as ICT is progressing[10]. Hence, building public awareness of cyber security requires an appropriate model of professional and university education[11]. On the other hand, expert knowledge possessed by those educated in this field and employed by public entities, should be used to understand and prevent cyber threats[12].

Exercising caution promotes improved security in cyberspace, especially in the age of widespread access to network services[13]. A high level of digital competence is desirable in society as a whole, yet particular care needs to be exercised in relation to those who, by virtue of their functions, have access to information, the disclosure of which may have negative consequences for the security of citizens or the state. This issue concerns, inter alia, data security (including personal data) in public administration, which is directly related to the security of citizens[14]. It should also be noted that when personal data is collected in an electronic form, its protection should be analysed not only from the perspective of the data subject but also from the perspective of state security[15]. It is therefore essential to manage cyber security, which consists in detection, assessment, counteraction and lessons for the future[16].

Detection of cyber threats is based not only on technical measures but also on the observation and analysis of online behaviour, including the activity of certain, often interconnected social media accounts or emerging fake news. Admittedly, in the case of the European Union's solutions, the problem of fake news is mostly not included in cyber security policy and is considered part of the

[10] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, p. 89.

[11] M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1, p. 48.

[12] Idem, *The obligations of public entities within the national cybersecurity system*, ibidem 2020, no. 2, p. 64.

[13] Idem, *Status prawny zespołów reagowania na incydenty bezpieczeństwa komputerowego w sferze cyberbezpieczeństwa* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. idem, Warszawa 2024, p. 163.

[14] E.M. Włodyka, *Samorządowa administracja publiczna wobec cyberprzestrzeni: bezpieczeństwo informacji a praktyka zgłaszania w samorządzie terytorialnym osób do kontaktu z CSIRT NASK*, „Studia Gdańskie. Wizje i Rzeczywistość" 2021, vol. 18, p. 302.

[15] J. Kurek, *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy big data. Aspekty prawne, organizacyjne i systemowe*, Warszawa 2021, p. 20–22.

[16] M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, „Prawo i Więź" 2023, no. 4, p. 10.

Member States' media systems[17]. However, it seems reasonable to argue that this phenomenon should be taken into account when managing cyber security. This is especially so since the global spread of false information and pervasive disinformation pose a serious threat to the functioning of a democratic society, including its cohesion, public health and political stability. A healthy democracy requires informed decisions based on truthful information. In contrast, false information has a negative impact on public beliefs about health, science, interculturalism or social issues. In addition to polarising and radicalising societies, false and manipulated content may lead to crisis situations[18].

The basis for the effectiveness of the perception of threat signals is that the relevant impacts are recognised in a timely manner, both on the side of causes (including their mechanisms of origin or transmission, as well as the mechanisms of their development) and their effects. In other words, knowledge of causal risks and the associated resultant risks is required[19]. As cyberspace is not an entity that is separate from the real world, some symptoms of cyber threats or cyber attacks can be perceived outside cyberspace. Similarly, signals of possible threats in the physical world can be spotted in cyberspace. This is particularly relevant in the context of the public sector's administration of critical infrastructures on the one hand and, on the other hand, huge amounts of data, collected as a rule from citizens on a mandatory rather than voluntary basis.

Electrical grids as an element of critical infrastructure risk

Critical infrastructure covers those systems that are essential to the proper functioning of society and the state, ones that include supplies of energy and energy resources, communication systems, ICT networks, financial systems, food supplies, drinking water supplies, health care, transport, emergency systems, systems to ensure continuity of public administration, production

[17] K. Wasilewski, *Fake News and the Europeanization of Cyberspace*, „Polish Political Science Yearbook" 2021, no. 4, p. 16.

[18] K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2, p. 19.

[19] B. Ćwik, *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review" 2017, no. 3, p. 30.

and storage of chemical and radioactive substances[20]. Critical infrastructure can be assumed to include the following areas: physical (physical components), process (management systems) and cyber (communication networks and control technologies)[21]. Of all the systems comprising critical infrastructure, the most important for the proper functioning of the economy and society is the system that supplies energy, energy raw materials and fuels. Without energy and, in particular, without a regular supply of energy raw materials and fuels, no other critical infrastructure element can function[22]. Critical infrastructures are inextricably linked to emergency management, because in the event of their failure, attacks on them or other incidents that disrupt their operation, appropriate procedures are triggered as part of emergency response[23].

It is also worth noting that the state's critical infrastructure includes those elements that function independently yet are interconnected. It is also influenced by ICT networks that exist in other states. These interdependencies make critical infrastructures vulnerable to cyber-attacks carried out both from within and outside a given country – virtually from all over the world[24]. Therefore, cyber protection of critical infrastructure is one of the key elements in ensuring its security. However, no matter how strongly an ICT network is secured, there is always a possibility of a successful cyber attack against it. Therefore, continuous threat monitoring is essential[25]. The increasing use of ICT in all the aspects of human activity also makes the functioning of critical infrastructure heavily reliant on network services. This, in turn, makes it increasingly vulnerable to various types of cyber attacks that can disrupt its functioning or even permanently damage its components. These attacks can be carried out using malware or using a distributed denial of service (DDoS). DDoS can disrupt network services, while malware can be used for espionage and sabotage actions aimed at stealing, modifying or destroying critical data.

[20] J. Kostrubiec, *Cybersecurity System in Poland. Selected Legal Issues* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022, p. 13.

[21] J. Procházka, P. Novobilsky, D. Procházkova, *Cyberbezpieczeństwo zarządzania sieciami i partycjami w transporcie kolejowym*, „Problemy Kolejnictwa" 2020, no. 189, p. 57.

[22] S. Dygantowski, *Cyberbezpieczeństwo jako fundament bezpieczeństwa infrastruktury krytycznej w kontekście współczesnych zagrożeń*, „Journal of KONBiN" 2020, no. 4, p. 310.

[23] R. Wódkiewicz, *Podstawowe zagrożenia funkcjonowania obiektów infrastruktury krytycznej*, „Zeszyty Naukowe SGSP" 2022, no. 83, p. 143.

[24] S. Woszek, *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, no. 14, p. 212.

[25] M. Barć, *Rodzaje ochrony infrastruktury krytycznej*, „Rocznik Bezpieczeństwa Morskiego" 2021, no. 15, p. 12.

Malware, supported by artificial intelligence algorithms, can also cause some critical infrastructure to malfunction by modifying the codes of the programs that control its operation.

Cyber attacks, including those on critical infrastructure, are most frequently made possible due to human error. They are often preceded by actions aimed at acquiring credentials to gain unauthorised access to the resources of the entity or person under attack. Attempts to distribute malware in order to gain secondary access to information systems, used to carry out further cybercriminal activities, also constitute an important aim of attacks[26].

Analyses showing the growing number of attacks on critical infrastructure are increasing. The phrase: „killware" is used to describe some of these. The term refers to the fact that such attacks target healthcare systems and can directly threaten human life. The threat from ransomware and other types of malware is not diminishing. Around the world, cybercriminals using malware disrupt hospitals, pipelines or sewage treatment plants. Worryingly, they are now focusing on such targets which, if attacked, could have a significantly negative impact on a large population[27]. Thus, it is enough if only one of the utilities, such as electricity, whose systems are also managed via ICT systems, easily succumbs to cyber-attacks in the absence of adequate protection in the form of auxiliary power supply.

Role of public administration and practice of electrical grid security

The inclusion of the electrical grid as part of cyber security systems raises the question of how to secure these and, as the first step, how to construct grid-integrated cyber security systems; this is a question concerning the normative basis. There is a variety of crisis management arrangements in place within the European Union in this area. In the Polish legislation, the Act of 26 April 2007 on crisis management[28] in Art. 2 indicates the domain of activity of

[26] *Więcej prób cyberataków na rządowe sieci i infrastrukturę krytyczną*, 2023, https://cyberdefence24.pl/cyberbezpieczenstwo/wiecej-prob-cyberatakow-na-rzadowe-sieci-i-infrastrukture-krytyczna [accessed: 25.03.2024].

[27] *Bezpieczeństwo infrastruktury krytycznej*, 2023, https://crn.pl/artykuly/bezpieczenstwo-infrastruktury-krytycznej-2/ [access: 25.03.2024].

[28] Act of 26 April 2007 on Crisis Management (Journal of Laws 2007, no. 89, item 590).

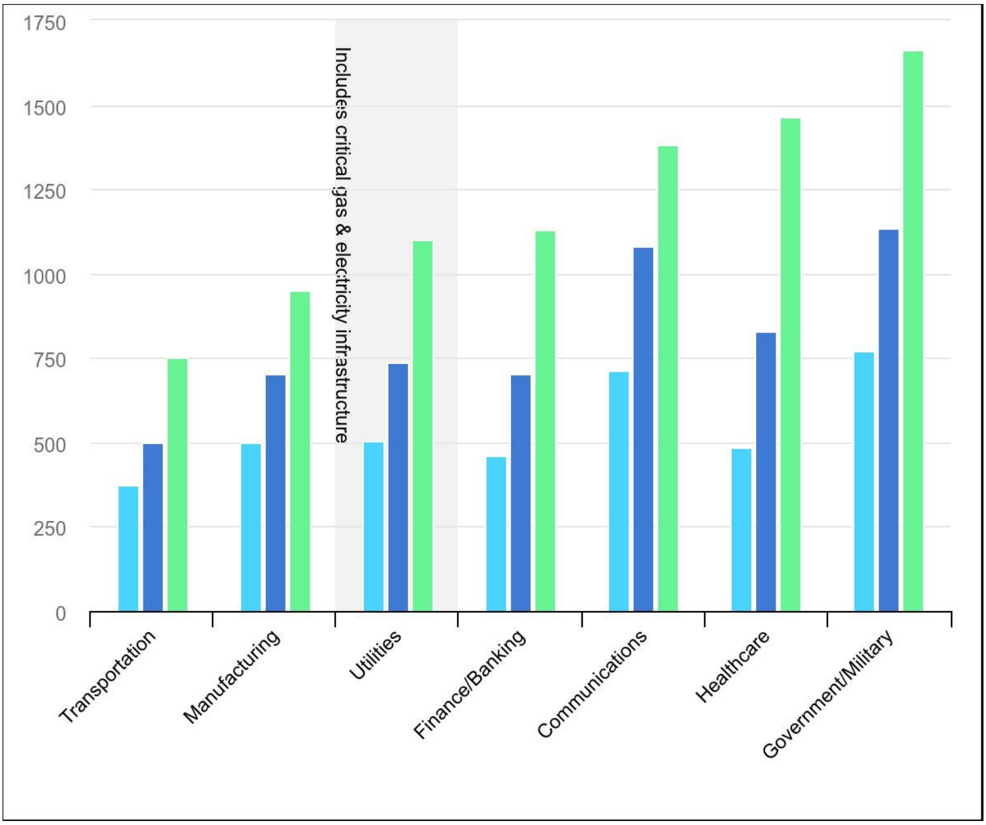
precisely public administration bodies in the area of crisis management, which constitutes an element of national security management. This activity consists in the prevention of emergencies, preparation to take control of these through planned action, responding to emergencies, recovering from them and restoring critical assets and infrastructure. In turn, Art. 3 para. 2, while providing a legal definition of „critical infrastructure", lists the systems it covers: these include, inter alia, energy, energy resources and fuel supply systems[29]. Under Art. 8 of the normative act referred to, the Government Crisis Management Team is established at the Council of Ministers, which is an opinion and advisory body that is competent in matters of initiation and coordination of actions taken in the area of crisis management. Meetings of the Team, as members, are attended by government administration bodies appointed by the Chairman, depending on the needs, including the minister in charge of the government administration department that is responsible for energy. Hence, there is an argument that supports the thesis concerning energy as being an area of security interest as a function of the state. In the situation of disruption of energy systems as a result of a cyber attack, an adequate state of emergency may be imposed if, through normal constitutional means, the government is unable to counter the threat, so it must take emergency measures[30].

Are the legal grounds referred to for securing cyber attacks reflected in practice? Unfortunately, the data covering the last two years leaves no doubt: current cyberattack trends pose an unprecedented threat to critical infrastructure, such as electricity systems. Cyberattacks are on the increase in the electricity sector, yet the IEA analysis indicates that utilities face serious difficulties in finding and retaining skilled professionals needed to defend themselves. There is increasing evidence that cyberattacks on utilities have been growing rapidly since 2018, reaching alarmingly high levels in 2022 following Russia's invasion of Ukraine. Recent cyberattacks in the electricity sector have disabled remote controls for wind farms, disrupted prepaid meters due to IT systems being unavailable, and led to recurrent data breaches

[29] Other elements of the critical infrastructure system include: communications systems, ICT networks, financial, food supply, water supply systems, health care, transport, rescue services, ensuring continuity of public administration, production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances.

[30] M. Karpiuk, *Zagrożenie bezpieczeństwa w cyberprzestrzeni jako przyczyna wprowadzenia stanu nadzwyczajnego*, „Studia Społeczne" 2023, no. 4, p. 209.

involving client names, addresses, bank account information and phone numbers. Worldwide, the average cost of a data breach hit a new record high in 2022, reaching USD 4,72 million in the energy sector[31].



Source: *Average number of weekly cyberattacks per organisation in selected industries, 2020–2022*, https://www.iea.org/data-and-statistics/charts/average-number-of-weekly-cyberattacks-per-organisation-in-selected-industries-2020-2022 [access: 20.03.2024].

Average number of weekly cyberattacks per organisation in selected industries, 2020–2022

As the research indicates, power grids as a component of cyber security are taken into consideration. In practice, scenarios with multiple events, such as the occurrence of both cyberattacks and failures of physical components, the occurrence of both cyberattacks and operators' (in)correct reactions,

[31] *Cybersecurity – is the power system lagging behind?*, https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind [access: 8.03.2024].

are considered and analysed. For each cyberattack scenario, Monte Carlo simulations are used to obtain possible sequences of the evolution of the system under study and then to derive risk estimates. As an application of the method proposed, the risk assessment method serves as the basis of risk-informed defence resource allocation to improve electric grid cybersecurity[32]. This is just an example of current research into the issue of cyber security of electrical grids and energy as part of such a system. However, a comprehensive and broader view is required considering the complexity of the issue, as it is not possible to consider only the IT and physical areas of cyber security systems. Nor is it only an area of normative regulation or the practice of research into cyber attack scenarios. Therefore, what is another element of the comprehensiveness of the system? The human factor must be taken into account here: the individual person's factor yet also the organisational culture within a particular institution or social group. Within the framework of the contribution offered by this study, it is difficult to make a clear argument as to whether it is organisational culture that has an impact on an enhancement of the cyber security system, or whether it is quite the opposite: it is the increasing level of technological development that forces the development of culture. In addition, given the extent of the expansion of public administration services in the area of e-government (administration whose functions are available to citizens online), lack of security for the continuity of electricity supply poses a significant challenge. The entire infrastructure does not need to be connected to the Internet for the system to succumb to cyber attacks. The argument seems to be justifiable that for such an attack to occur (on the supply of electricity to a specific public administration institution) it would be sufficient if it was the electricity management system that was connected to the Internet, if only through the power plant's power transmission management system.

Conclusions

Cyber attacks on electrical grids may have catastrophic consequences, ones that may undoubtedly pose a threat not only to state security but to human health, as well, and this definitely applies not only to cyberspace but, above all, to the real world. The study, which constitutes a contribution to

[32] X. Diao et al., op. cit.

a comprehensive analysis of the issue of the cyber security of electrical grids and the participation of the public administration in this system, did not cover numerous aspects that deserve a separate study. Among other things, the following research questions were not answered:

– How do national and EU public policies address the cyber security of the aforementioned sector?

– Is it a complementary system, one that is included in international cooperation?

– In what ways is the energy sector vulnerable to cyber attacks; what is the weakest link in cyber security systems?

– In addition to technical aspects, and taking into account the human factor, how can a streamlined organisational culture of the personnel of public administrations and public entities contribute to an increased cyber security of electrical grids?

– Are there any scenarios within crisis management for public entities that could anticipate the consequences and increase security in the event of a cyber attack on electrical grids?

– What should be the role of the state and public administration in helping to ensure the cyber security of these grids in relation to the lives, health and safety of citizens?

These are only examples of research questions that require further study. However, the paper draws attention to the predominance of research that analyses the issue under discussion from a purely technical perspective, while not paying enough research attention to the human factor or organisational culture. Thus, the research hypothesis was confirmed indicating an urgent need for a comprehensive approach to the cyber security policy of electrical grids in a broader perspective, not only the technical one but also taking into account the public policies of states and the human factor.

The area affected by risks related to cyber attacks is greater than just the location of a power plant. Every element of the electric power grid system is potentially vulnerable to attacks: at the stage of energy transmission, the distribution grid and supply chain partners. Cyber security in this respect should also take into account theft of data from the grid or ransomware. Additionally, increased digitisation of power grid raises questions as to weaknesses in the cybersecurity of smart grids. As a contribution to research, the article therefore indicates the successive steps in the development in this area.

Bibliography

Average number of weekly cyberattacks per organisation in selected industries, 2020-2022, https://www.iea.org/data-and-statistics/charts/average-number-of-weekly-cyberattacks-per-organisation-in-selected-industries-2020-2022 [access: 20.03.2024].

Barć M., *Rodzaje ochrony infrastruktury krytycznej*, „Rocznik Bezpieczeństwa Morskiego" 2021, no. 15.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

Bencsik A., Karpiuk M., *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

Bezpieczeństwo infrastruktury krytycznej, 2023, https://crn.pl/artykuly/bezpieczenstwo-infrastruktury-krytycznej-2/ [access: 25.03.2024].

Ćwik B., *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review" 2017, no. 3.

Cybersecurity – is the power system lagging behind?, https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind [access: 8.03.2024].

Diao X., Zhao Y., Smidts C., Vaddi P. K., Li R., Lei H., Chakhchoukh Y., Johnson B., Le Blanc K., *Dynamic probabilistic risk assessment for electric grid cybersecurity*, „Reliability Engineering & System Safety" 2024, no. 109699.

Dygantowski S., *Cyberbezpieczeństwo jako fundament bezpieczeństwa infrastruktury krytycznej w kontekście współczesnych zagrożeń*, „Journal of KONBiN" 2020, no. 4.

Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2.

Kaczmarek K., Włodyka E., *Strategiczne znaczenie Cieśniny Ormuz i jego implikacje dla bezpieczeństwa energetycznego Europy w kontekście agresji Rosji na Ukrainę*, „Studia Gdańskie. Wizje i Rzeczywistość" 2022, vol. 19.

Karpiuk M., *Crisis management vs. cyber threat*, "Sicurezza, terrorismo e società" 2022, no. 2.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., Makuch A., Soler U., *The Role of the Cybersecurity Strategy of the Republic of Poland in Ensuring Cybersecurity*, „Polish Political Science Yearbook" 2023, no. 3.

Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, „Prawo i Więź" 2023, no. 4.

Karpiuk M., *Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2.

Karpiuk M., *Status prawny zespołów reagowania na incydenty bezpieczeństwa komputerowego w sferze cyberbezpieczeństwa* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024.

Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no, 2.

Karpiuk M., *Zagrożenie bezpieczeństwa w cyberprzestrzeni jako przyczyna wprowadzenia stanu nadzwyczajnego*, „Studia Społeczne" 2023, no. 4.

Kostrubiec J., *Cybersecurity System in Poland. Selected Legal Issues* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Kostrubiec J., *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland*, „Lex Localis – Journal of Local Self-Government" 2021, no. 1.

Kurek J., *Bezpieczeństwo Państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy big data. Aspekty prawne, organizacyjne i systemowe*, Warszawa 2021.

Procházka J., Novobilsky P., Procházkova D., *Cyberbezpieczeństwo zarządzania sieciami i partycjami w transporcie kolejowym*, „Problemy Kolejnictwa" 2020, no. 189.

Wasilewski K., *Fake News and the Europeanization of Cyberspace*, „Polish Political Science Yearbook" 2021, no. 4.

Więcej prób cyberataków na rządowe sieci i infrastrukturę krytyczną, 2023, https://cyberdefence24.pl/cyberbezpieczenstwo/wiecej-prob-cyberatakow-na-rzadowe-sieci-i-infrastruktura-krytyczna [access: 25.03.2024].

Włodyka E.M., *Samorządowa administracja publiczna wobec cyberprzestrzeni: bezpieczeństwo informacji a praktyka zgłaszania w samorządzie terytorialnym osób do kontaktu z CSIRT NASK*, „Studia Gdańskie. Wizje i Rzeczywistość" 2021, vol. 18.

Wódkiewicz R., *Podstawowe zagrożenia funkcjonowania obiektów infrastruktury krytycznej*, „Zeszyty Naukowe SGSP" 2022, no. 83.

Woszek S., *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, no. 14.

Cyberbezpieczeństwo sieci elektroenergetycznych – przyczynek do badań

Streszczenie

Infrastruktura krytyczna państwa to elementy, które funkcjonują samodzielne, lecz są ze sobą połączone. Wpływ na nią mają również sieci teleinformatyczne istniejące w innych państwach. Te zależności powodują, że infrastruktura krytyczna jest w sposób szczególny narażona na ataki cybernetyczne. Jednocześnie najbardziej krytycznym elementem infrastruktury krytycznej są sieci elektroenergetyczne. Hipoteza badawcza zakłada pilną potrzebę kompleksowego ujęcia polityki cyberbezpieczeństwa sieci elektroenergetycznych w szerszej perspektywie, nie tylko tej technicznej, lecz także uwzględniającej polityki publiczne i czynnik ludzki. W celu weryfikacji tej hipotezy zostały zastosowane metody: ilościowa, jakościowa, badanie literatury przedmiotu oraz metoda *desk research*.

Analizy przeprowadzone przez autorów w sposób jednoznaczny pokazały, że najbardziej podatnym na cyberzagrożenia elementem infrastruktury krytycznej są sieci elektroenergetyczne.

Słowa kluczowe: sieci elektroenergetyczne, administracja publiczna, cyberbezpieczeństwo, infrastruktura krytyczna