Articles Studia Iuridica Lublinensia vol. XXX, 2, 2021
DOI: 10.17951/sil.2021.30.2.233-244

Mirosław Karpiuk
University of Warmia and Mazury in Olsztyn, Poland
ORCID: 0000-0001-7012-8999
miroslaw.karpiuk@uwm.edu.pl

Organisation of the National System of Cybersecurity: Selected Issues

Organizacja krajowego systemu cyberbezpieczeństwa. Wybrane zagadnienia

ABSTRACT

The issues discussed in this paper concern cybersecurity. The threats present in cyberspace are becoming increasingly difficult to detect, and their prevention requires not only knowledge and special equipment, but also considerable financial resources. As such, the State has to put a great deal of effort (both institutional and financial) into cybersecurity measures directed against attacks. In order to meet the challenges connected with ensuring cybersecurity, the legislators have undertaken the regulation of such issues by adopting laws on the national cybersecurity system to allow the responsible authorities to properly secure cyberspace against threats. As part of the national cybersecurity system, lawmakers have imposed a number of obligations on public entities to ensure that information systems are resistant to actions which compromise the confidentiality, integrity, accessibility, and authenticity of processed data, and the related services offered by such systems. Appropriate obligations have also been exacted on the operators of essential services (OES), i.e. services key to maintaining critical social or economic activities which are included in the list of essential services.

Keywords: cybersecurity; information systems; cyberspace; essential services; national cybersecurity system

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, PhD., dr. habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, Obitza 1, 10-725 Olsztyn, Poland.

INTRODUCTION

Security is an area of considerable concern to the state. Ensuring freedom from threats, or rendering such threats harmless to the normal functioning of public institutions, private entities, or society (ensuring security), is the primary objective of each state. There are multiple levels at which this objective should be met. Effective protection against threats allows the state to fulfil its public mission of meeting the needs of society (including its security needs) and supporting its development.

One of the actors in the national cybersecurity system is local government.[1] Local governments are separate decentralised authorities which perform public tasks, have their own governing bodies and the attribute of independence, and act on local or regional scales to exercise their competences in their own name and at their own responsibility. It should be noted, however, that the legislators have not provided local governments with the instruments they need to properly perform their cybersecurity tasks, as these are largely managed by State institutions.

Cybersecurity is one of the domains of any country's security. It is all the more important today, and the repercussions of cybersecurity breaches affect not only public spaces but also the social sphere. Therefore, the State must respond quickly and decisively to cyberattacks, while seeking more and more advanced protection mechanisms. In their efforts to react to the increasingly frequent threats to cyberspace, the Polish legislators decided to introduce an appropriate regulation which would allow an accurate diagnosis and a sufficient response in the event of a cyberattack.

The aim of the national cybersecurity system is to ensure cybersecurity at the national level, entailing the uninterrupted provision of both essential and digital services, which is to be achieved by guaranteeing a proper level of security within information systems used to provide such services, as well as by providing smooth incident-management procedures.[2] The lawmakers have not provided any exact definition of the system, and have specified it only through certain statutory determinants (including the purpose), which makes it difficult to define its overall status. The system of cybersecurity should indeed work as a system, i.e. as a group of synchronised institutional and functional components which deploy their relevant skills and know-how to perform specific tasks. This system should be composed of various cybersecurity-related entities, organised into one interconnected whole, and equipped with the appropriate tools. The current solution undoubtedly lacks cohe-

[1] 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, vol. 19(1), p. 115.

[2] Article 3 of the Act of 5 July 2018 on the Polish National Cybersecurity System (Journal of Laws 2018, item 1560 as amended), hereinafter: NCSA.

sion. However, when postulating further work aimed at optimising legal measures in this field, one should treat it as a springboard for a satisfactory system designed to ensure the country's cybersecurity.

Pursuant to Article 3 NCSA, the overarching goal of the national cybersecurity system is to ensure cybersecurity at the national level by means of the uninterrupted provision of both essential and digital services, and proper incident-management procedures. It seems that the legislators have misused the term "ensure" when it comes to cybersecurity, thus downplaying the essence of potential threats which could disable the system. Lawmakers should know that it is not always possible to ensure cybersecurity, particularly in the age of such intense technological advancement. Given the existing level of the legal regulations, and the technical and financial possibilities, the activities of the national cybersecurity system are rather to protect, not to secure (in the absolute meaning of the term "ensure" as used in the NCSA).

The aim of this paper is to provide a general description of the national cybersecurity system in Poland.

THE ENTITIES IN THE NATIONAL CYBERSECURITY SYSTEM

As indicated by Article 4 NCSA, the national cybersecurity system is comprised of the following entities:[3] 1) the operators of essential services; 2) digital-services providers; 3) CSIRT MON (the national-level Computer Security Incident Response Team under the Minister of National Defence, as stipulated in Article 2 para. 2 NCSA); 4) CSIRT NASK (the national-level Computer Security Incident Response Team, headed by NASK – Research and Academic Computer Network – the National Research Institute, as stipulated in Article 2 para. 3 NCSA); 5) CSIRT GOV (the national-level Computer Security Incident Response Team, under the Head of the Internal Security Agency, as stipulated in Article 2 para. 1 NCSA); 6) sectoral cybersecurity teams; 7) selected public-finance entities, referred to in Article 9 points 1–6, 8, 9, 11 and 12 of the Polish Act of 27 August 2009 on public finance (Journal of Laws 2019, item 869 as amended);[4] 8) research institutes;

[3] K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021, p. 4.

[4] These public finance sector entities are: 1) public administration bodies, including the government administration, institutions of state inspection and law enforcement, courts and tribunals; 2) local-government units and their associations; 2a) metropolitan associations; 3) budgetary entities; 4) local-government budgetary bodies; 5) executive agencies; 6) public-sector enterprises; 8) the Social Insurance Institution, including any funds under its management, and the Agricultural Social Insurance Funds, including any funds under the management of its President; 9) the National Health Fund; 11) public tertiary institutions; 12) the Polish Academy of Sciences, including any organisational units it might establish. Public finance entities also cover local-government units operating in

9) the National Bank of Poland;[5] 10) the National Development Bank;[6] 11) the Office for Technical Inspection;[7] 12) the Polish Air Navigation Services Agency;[8] 13) the Polish Centre for Accreditation;[9] 14) the National Fund for Environmental Protection and Water Management, and regional funds for environmental protection and water management;[10] 15) commercial companies and partnerships in charge of public services;[11] 16) entities which provide cybersecurity services; 17) authorities

many fields, including telecommunications. For more details, see M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, "Cybersecurity and Law" 2019, no. 1, pp. 37–45; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, "Cybersecurity and Law" 2019, no. 2, pp. 39–48.

[5] The National Bank of Poland (NBP) is the central bank of the State. It has the exclusive right to issue money and to define and implement monetary policy. The National Bank of Poland is responsible for the value of the Polish currency (Article 227 para. 1 of the Constitution of the Republic of Poland of 2 April 1997, Journal of Laws 1997, no. 78, item 483 as amended; English translation of the Constitution at www.sejm.gov.pl/prawo/konst/angielski/kon1.htm [access: 10.05.2021]). Article 227 of the Constitution of the Republic of Poland consolidates the independence of the National Bank of Poland, gives it stronger guarantees, and strengthens its new competences (see M. Bartoszewicz, *Komentarz do art. 227*, [in:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, ed. M. Haczkowska, LEX/el. 2014). The main objective of the National Bank of Poland is to maintain prices at a stable level, while supporting the central economic policy, as long as it does not limit the Bank's primary goal (Article 3 para. 1 of the Polish Act of 29 August 1997 on the National Bank of Poland, consolidated text Journal of Laws 2019, item 1810).

[6] The National Development Bank is a State bank headquartered in the capital city of Warsaw (Article 2 para. 1–2 of the Polish Act of 14 March 2003 on National Development Bank, consolidated text Journal of Laws 2018, item 1543 as amended).

[7] The Office for Technical Inspection was established as a State legal entity headquartered in the capital city of Warsaw (Article 35 of the Polish Act of 21 December 2000 on technical inspection, consolidated text Journal of Laws 2019, item 667 as amended).

[8] The Polish Air Navigation Services Agency is established as a State legal entity, headquartered in Warsaw (Article 1 of the Polish Act of 8 December 2006 on the Polish Air Navigation Services Agency, consolidated text Journal of Laws 2017, item 1976).

[9] The Polish Centre for Accreditation is the State's accreditation body, and, at the same time, a State legal entity supervised by the Minister responsible for the economy (Article 38 of the Polish Act of 13 April 2016 on conformity assessment and market surveillance systems, consolidated text Journal of Laws 2019, item 544).

[10] The National Fund for Environmental Protection and Water Management is a State legal person, while the regional funds for environmental protection and water management are local government legal persons (Article 400 of the Polish Act of 27 April 2001 – Environmental Protection Law, consolidated text Journal of Laws 2019, item 1396 as amended). Environmental protection is a domain that requires significant capital expenditure. Therefore, it cannot exist without relevant financial solutions. The Polish lawmakers have decided that measures aimed at improving the condition of the environment will be financed with funds for environmental protection and water management. See K. Gruszecki, *Komentarz do art. 400*, [in:] idem, *Prawo ochrony środowiska. Komentarz*, LEX/el. 2019.

[11] The aim of public service tasks performed by commercial companies and partnerships as part of the national cybersecurity system is to meet, continuously and uninterruptedly, the collective society needs by providing publicly accessible services, which stems from Article 1 para. 2 of the

in charge of cybersecurity; 18) the Single Point of Contact for cybersecurity; 19) the Government's Plenipotentiary for Cybersecurity; 20) the Cybersecurity Board. Therefore, the legislators chose those entities which they believed played a vital role in the cybersecurity system, and also those being important from the point of view of the strategic interests of the country, including in the field of telecommunications.

THE OBLIGATIONS OF THE OPERATORS OF ESSENTIAL SERVICES

The EU legislators expressly stipulate that Member States are to take steps in order to ensure that the operators of essential services implement appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. When doing so, they should factor in the latest state of the art. Their protection measures must ensure a level of network and information-systems security which corresponds to the risks posed. Furthermore, EU Member States are to ensure that the operators of essential services take the appropriate measures to prevent or minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, which aims to ensure the continuity of such services. Member States also need to ensure that the operators of essential services immediately notify the responsible authority or the CSIRT of incidents with a significant impact on the continuity of the essential services they provide. Such notifications have to include information enabling the responsible authority or CSIRT to determine any cross-border impact of the incident, while at the same time they cannot make the notifying party subject to increased liability.[12]

Pursuant to Article 8 NCSA, the operators of essential services are required to deploy a security-management system within the information systems they use to provide their services. Such a security-management system is to ensure the following: 1) regular incident-risk assessment and risk management; 2) the implementation of the appropriate technical and organisational measures proportionate to the assessed risk, taking into account the latest state of the art, including a) the maintenance and safe operation of the information system, b) physical and environmental security, including access control, c) the security and continuity of services key to the provision of the essential service, d) the deployment, record-keeping, and maintenance of action plans which allow the continuous and uninterrupted provi-

Polish Act of 20 December 1996 on municipal management (consolidated text Journal of Laws 2019, item 712 as amended).

[12] Article 14 of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1).

sion of the essential service, and ensure the confidentiality, integrity, availability, and authenticity of information, e) the implementation of a continuous monitoring system to supervise the information system used to provide the essential service; 3) the collecting of information on cybersecurity threats and the vulnerabilities of the information system used to provide the essential service; 4) incident management; 5) the applying of measures to prevent and minimise the impact of incidents on the security of the information system used to provide the essential service, including a) using mechanisms to ensure the confidentiality, integrity, availability, and authenticity of the data processed in the information system, b) keeping the software up to date, c) security measures against unauthorised modification in the information system, d) taking immediate action on identifying a vulnerability or a cybersecurity threat; 6) using the means of communication which facilitate accurate and safe communication within the national cybersecurity system.

The obligations imposed on the operators of essential services include the following basic activities and processes: risk management, with the implementation of physical, technical, and organisational security measures based on risk assessment; incident management, and the management of effective incident responses; and an obligation to guarantee a safe and secure communication channel operating within the national cybersecurity system.[13]

The obligations of the operators of essential services (OES) involve many fields, including incident-risk assessment and incident-risk management, and finally incident management. Risk assessment should be understood as the overall process of risk identification, analysis, and estimation (Article 2 para. 13 NCSA); an incident is defined as an event which has or might have an adverse effect on cybersecurity (Article 2 para. 5 NCSA); and risk management entails coordinated activities in the sphere of cybersecurity management in relation to the assessed risk (Article 2 para. 19 NCSA). Incident management means handling an incident, searching for connections between incidents, eliminating incident causes, and developing conclusions drawn from incident handling (Article 2 para. 18 NCSA).

As stated in Article 9 NCSA, the operator of essential services: 1) designates a person responsible for communicating with entities in the national cybersecurity system; 2) provides essential-service users with access to knowledge which allows them to understand cybersecurity threats and employ effective precautions against such threats within the scope associated with the essential services provided, in particular by publishing relevant information on the operator's website; 3) provides the responsible authority with relevant data no later than within 3 months of changing the data.

[13] K. Świtała, *Komentarz do art. 8*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, LEX/el. 2019.

A public administration body may designate a contact person using whatever legal form available. It is not obliged to perform a strictly defined legal act resulting in the appointment of a contact person who will communicate with the entities of the national cybersecurity system.

The OES are required to fulfil their information obligations towards the person who is the user of this type of service. The exchange of relevant messages may take place *via* the operator's website; there is no requirement to send such personalised information directly by electronic means, such as e-mail.[14]

Further obligations of the OES are set out in Article 11 NCSA. Under this provision, the OES should: 1) ensure incident handling; 2) provide access to information on recorded incidents to the responsible CSIRT MON, CSIRT NASK, or CSIRT GOV, to the extent which is necessary for the operators to perform their tasks; 3) classify incidents' seriousness, based on the incident seriousness thresholds; 4) report serious incidents immediately, and not later than within 24 hours from detection, to the responsible CSIRT MON, CSIRT NASK, or CSIRT GOV; 5) cooperate with the responsible CSIRT MON, CSIRT NASK, or CSIRT GOV during the handling of serious and critical incidents by, e.g., providing the required data, including personal data; 6) remove the vulnerability which has caused or could potentially cause a severe, significant, or critical incident, and notify the responsible authority of its having eliminated the vulnerability. As part of the obligations set out in Article 11 NCSA, two terms have been described – "serious incident" and "critical incident". A serious incident is an event which causes or might cause a serious reduction in the quality of, or discontinuity in, the provision of the essential services (Article 2 para. 7 NCSA); a critical incident is an occurrence leading to significant damage to public safety[15]

[14] Idem, *Komentarz do art. 9*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa…*

[15] For more on security and safety, see M. Czuryk, J. Kostrubiec, *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, vol. 41(1), pp. 33–47; M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2, pp. 67–70; M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, no. 3, p. 15; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013, pp. 77–89; idem, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, vol. 26(4), p. 10; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018, p. 7; M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014, pp. 28–34; J. Kostrubiec, *Status of a Voivodship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, no. 5, pp. 35–40; M. Karpiuk, J. Kostrubiec, *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, vol. 27(2), p. 65; D. Tyrawa, *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym*, Lublin 2018, pp. 40–46; K. Bojarski, *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-*

or public order,[16] international interests, economic interests, the operations of public institutions, civil rights and freedoms, or human lives and health, as classified by the responsible CSIRT MON, CSIRT NASK, or CSIRT GOV (Article 2 para. 6 NCSA).

THE RESPONSIBLE CYBERSECURITY AUTHORITIES

In Article 41 NCSA, the lawmakers define a catalogue of authorities in charge of cybersecurity, including: 1) for the energy sector – the Minister responsible for energy; 2) for the transportation sector, excluding the water-transportation sub-sector – the Minister responsible for transportation; 3) for the water-transportation sub-sector – the Minister responsible for the maritime economy and the Minister responsible for inland navigation; 4) for the banking sector and the financial-market infrastructure – the Polish Financial Supervision Authority 5) for the healthcare sector – the Minister responsible for healthcare; 6) for the healthcare sector, the digital infrastructure sector, and digital-service providers, including the following entities – a) entities subsidiary to, or supervised by, the Minister of National Defence, including organisations whose ICT systems or ICT networks are included in a uniform specification of sites, installations, facilities and services forming a part of the critical infrastructure[17] – the Minister of National Defence, b) entrepreneurs of special economic and defence significance for which the Minister of National Defence coordinates and supervises the performance of national defence tasks[18] – the Minister of National Defence; 7) for the drinking-water supply and distribution

-prawnym, Warszawa–Nisko 2017, pp. 19–72; K. Chałubińska-Jentkiewicz, M. Karpiuk, K. Zalasińska, *Prawo bezpieczeństwa kulturowego*, Siedlce 2016, p. 7.

[16] For more information on public order, see M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017, pp. 14–21; K. Chałubińska-Jentkiewicz, *Moralność publiczna w polskim prawie gospodarczym i w prawie mediów*, [in:] *Klauzule porządku publicznego i moralności publicznej*, eds. G. Blicharz, M. Delijewski, Warszawa 2019, pp. 244–245; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017, pp. 96–102; A. Pieczywok, *Służba w formacjach bezpieczeństwa i porządku publicznego*, eds. M. Karpiuk, A. Pieczywok, Warszawa 2016, p. 10; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, vol. 9, p. 11.

[17] This is a uniform list of facilities, installations, devices, and services included in the critical infrastructure broken down into systems. The list also includes the European critical infrastructure located on the territory of the Republic of Poland, and the European critical infrastructure located on the territory of other EU Member States which might have a significant impact on the Republic of Poland. The list is classified, see Article 5b para. 7 point 1 of the Polish Act of 26 April 2007 on crisis management (consolidated text Journal of Laws 2019, item 1398).

[18] The list of entrepreneurs of special economic and defence significance was established by the legislators in the Regulation of the Council of Ministers of 3 November 2015 on the list of entrepreneurs of special economic and defence significance (Journal of Laws 2015, item 1871 as amended).

sector – the Minister responsible for water management; 8) for the digital-infrastructure sector and for digital-service providers – the Minister responsible for computerisation.

The Polish legislators have decided to create a dispersed model of cybersecurity-responsible authorities, with several authorities performing this function and dealing with matters substantially related to the specific nature of the activities of the operators of essential services, and of digital-service providers.[19]

CONCLUSION

According to the EU legislators, ICT networks, systems, and services play a vital role in society, which is indeed very true. The reliability and security of such networks, systems, and services are of utmost importance for both the economic and social spheres, in particular for the well-being of the internal market. The scale, frequency, and impact of security incidents are on the rise, posing a serious threat to the functioning of network and information systems. Information systems can also become the target of malicious acts aimed at damaging or disrupting their operations. Such incidents can not only impede business operations, but also generate significant financial losses, undermine the confidence of users, and result in serious losses to the economy of the EU and its Member States. Responding effectively to challenges to the security of network and information systems, therefore, requires a global approach at the Union level covering common minimum capacity building and planning requirements, the exchange of information, cooperation, and common security requirements for the operators of essential services and digital service providers.[20]

The dynamic civilisation shifts of recent years stem from the rapid advancement of information techniques and information and communication technologies. Cyberspace is only one of the new spheres in which these processes take place.[21] This field should be properly secured, because it is of strategic importance, not only for the proper functioning of the country itself, but also for the information society, which needs and uses various forms of communication.

Ensuring cybersecurity, which is intended to be achieved through systemic measures, relates to the protection of information systems' integrity against unau-

[19] K. Prusak-Górniak, K. Silicki, *Komentarz do art. 41*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa…*

[20] An Introduction to Directive (EU) 2016/1148.

[21] K. Chałubińska-Jentkiewicz, *Odpowiedzialność w sieci – diagnoza stanu obecnego*, [in:] *System bezpieczeństwa w cyberprzestrzeni RP*, eds. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, Warszawa 2018, p. 13.

thorised interference. The job of information systems is to guarantee the uninterrupted exchange of data *via* telecommunications networks, and the uninterrupted provision of digital services. Such protection is the responsibility of the State. It is the State which should foster the optimal conditions (including the legal conditions) for successful cybersecurity.[22]

The issues related to security in cyberspace are determined by the development of new technologies, including robotics, as well as digital processes and the ever-evolving computerisation. The progress of the State's computerisation is a key building block in the development of cybersecurity administration, which should be perceived in two dimensions. The first involves a specific group of institutions with the appropriate powers and functions in the sphere of cybersecurity administration. The second dimension is related to the domain of the law, which is used to implement the State's cybersecurity-related mission, goals, and tasks, at both national and international levels.[23]

REFERENCES

Literature

Bartoszewicz M., *Komentarz do art. 227*, [in:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, ed. M. Haczkowska, LEX/el. 2014.

Bojarski K., *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-prawnym*, Warszawa–Nisko 2017.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Chałubińska-Jentkiewicz K., *Moralność publiczna w polskim prawie gospodarczym i w prawie mediów*, [in:] *Klauzule porządku publicznego i moralności publicznej*, eds. G. Blicharz, M. Delijewski, Warszawa 2019.

Chałubińska-Jentkiewicz K., *Odpowiedzialność w sieci – diagnoza stanu obecnego*, [in:] *System bezpieczeństwa w cyberprzestrzeni RP*, eds. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, Warszawa 2018.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021.

[22] I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, "Cybersecurity and Law" 2020, vol. 2(4), p. 200.

[23] K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, p. 16. For more on new technologies, see K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015. For more on cybersecurity, see A. Pieczywok, *Cyber threats and challenges targeting man versus his education*, "Cybersecurity and Law" 2019, no. 1.

Chałubińska-Jentkiewicz K., Karpiuk M., Zalasińska K., *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, no. 3.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, "Cybersecurity and Law" 2019, no. 2.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Czuryk M., Kostrubiec J., *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, vol. 41(1), **DOI: https://doi.org/10.19195/2300-7249.41.1.3**.

Gruszecki K., *Komentarz do art. 400*, [in:] idem, *Prawo ochrony środowiska. Komentarz*, LEX/el. 2019.

Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, "Cybersecurity and Law" 2020, vol. 2(4).

Karpiuk M., *Activities of the local government units in the scope of telecommunication*, "Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, vol. 26(4), **DOI: http://dx.doi.org/10.17951/sil.2017.26.4.9**.

Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.

Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, vol. 9.

Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2.

Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.

Karpiuk M., Kostrubiec J., *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, vol. 27(2), **DOI: https://doi.org/10.17951/sil.2018.27.2.65**.

Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.

Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.

Kostrubiec J., *Status of a Voivodship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, no. 5.

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, vol. 19(1), **DOI: https://doi.org/10.4335/19.1.111-129(2021)**.

Pieczywok A., *Cyber threats and challenges targeting man versus his education*, "Cybersecurity and Law" 2019, no. 1.

Pieczywok A., *Profesjonalność funkcjonariuszy wybranych służb w obszarze bezpieczeństwa i porządku publicznego*, [in:] *Służba w formacjach bezpieczeństwa i porządku publicznego*, eds. M. Karpiuk, A. Pieczywok, Warszawa 2016.

Prusak-Górniak K., Silicki K., *Komentarz do art. 41*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, LEX/el. 2019.

Świtała K., *Komentarz do art. 8*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, LEX/el. 2019.

Świtała K., *Komentarz do art. 9*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, LEX/el. 2019.

Tyrawa D., *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym*, Lublin 2018.

Legal acts

Act of 20 December 1996 on municipal management (consolidated text Journal of Laws 2019, item 712 as amended).
Act of 27 August 2009 on public finance (Journal of Laws 2019, item 869 as amended).
Act of 29 August 1997 on the National Bank of Poland (consolidated text Journal of Laws 2019, item 1810).
Act of 21 December 2000 on technical inspection (consolidated text Journal of Laws 2019, item 667 as amended).
Act of 27 April 2001 – Environmental Protection Law (consolidated text Journal of Laws 2019, item 1396 as amended).
Act of 14 March 2003 on National Development Bank (consolidated text Journal of Laws 2018, item 1543 as amended).
Act of 8 December 2006 on the Polish Air Navigation Services Agency (consolidated text Journal of Laws 2017, item 1976).
Act of 26 April 2007 on crisis management (consolidated text Journal of Laws 2019, item 1398).
Act of 13 April 2016 on conformity assessment and market surveillance systems (consolidated text Journal of Laws 2019, item 544).
Act of 5 July 2018 on the Polish National Cybersecurity System (Journal of Laws 2018, item 1560 as amended).
Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483 as amended).
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1).
Regulation of the Council of Ministers of 3 November 2015 on the list of entrepreneurs of special economic and defence significance (Journal of Laws 2015, item 1871 as amended).

ABSTRAKT

Podjęta w artykule problematyka dotyczy cyberbezpieczeństwa. Zagrożenia występujące w cyberprzestrzeni stają się coraz trudniejsze do wykrycia, a przeciwdziałanie im wymaga nie tylko wiedzy i sprzętu specjalistycznego, lecz także znacznych nakładów finansowych. W związku z powyższym państwo musi wkładać istotny wysiłek w działania zabezpieczające cyberprzestrzeń przed atakami (zarówno instytucjonalny, jak i finansowy). Wychodząc naprzeciw wyzwaniom związanym z zapewnieniem cyberbezpieczeństwa, ustawodawca podjął się uregulowania tego rodzaju kwestii, uchwalając ustawę o krajowym systemie cyberbezpieczeństwa, która ma pozwalać właściwym podmiotom na odpowiednie zabezpieczenie cyberprzestrzeni przed zagrożeniami. W ramach krajowego systemu cyberbezpieczeństwa nakłada się na poszczególne podmioty szereg obowiązków, które są związane z zapewnieniem odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Ustawodawca stosowne obowiązki nałożył również na operatorów usług kluczowych, czyli usług, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienione w wykazie usług kluczowych.

Słowa kluczowe: cyberbezpieczeństwo; systemy informacyjne; cyberprzestrzeń; usługi kluczowe; krajowy system cyberbezpieczeństwa