Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

Articles

Studia Iuridica Lublinensia vol. 32, 5, 2023
DOI: 10.17951/sil.2023.32.5.43-52

Małgorzata Czuryk
University of Warmia and Mazury in Olsztyn, Poland
ORCID: 0000-0003-0362-3791
malgorzata.czuryk@uwm.edu.pl

Cybersecurity and Protection of Critical Infrastructure

Cyberbezpieczeństwo a ochrona infrastruktury krytycznej

ABSTRACT

The functioning of critical infrastructure depends on information and communication technologies (ICT) systems that enable its equipment or facilities to operate smoothly. Threats to its functioning can present a major issue for the state and society, as it also spans strategic sectors which overlap with the essential services which remain within the purview of operators of essential services. Because of the relationship that links strategic systems within critical infrastructure and simultaneously supports its operation with essential services, ensuring cybersecurity will also affect the protection of this infrastructure. It should be emphasised that critical infrastructure may be adequately protected by ensuring the cyber resilience of the ICT systems it utilises and through cooperation between the public and the private sector.

Keywords: cybersecurity; cyberspace; crisis management; critical infrastructure

INTRODUCTION

Cyber threats can lead to various adverse phenomena and provoke crises, particularly when cyberattacks target information and communication technologies (ICT) systems, including those involved in the uninterrupted functioning of critical infrastructure. Threats in cyberspace may result in contingencies, given that public institutions and private entities are highly computerised while the ICT systems they

CORRESPONDENCE ADDRESS: Małgorzata Czuryk, PhD, Dr. Habil., University Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Dybowskiego 13, 10-723 Olsztyn, Poland.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

rely on are not always properly secured.[1] Such ICT systems can also ensure the continual operation of critical infrastructure facilities.

For critical infrastructure to function properly, cyberspace is utilised: a domain where information is processed and exchanged across ICT systems, encompassing the links between the latter and the relations with users.[2] Cyberspace is a global network formed by interconnected ICT networks, which comprise devices that enable information to be generated, processed, and exchanged between such devices either automatically or knowingly, as well as intentionally between their users. Cyberspace, thus defined as an area of daily activity for states and citizens pursuing their vital interests, is constantly under threat, not only due to illegal actions of individuals or groups but also because of system errors or failures.[3]

It should be stressed that the local government is the first tier responsible for crisis management, whose tasks include preventing contingencies, preparing for taking control of such events, mitigating their aftermath, and restoring the resources and critical infrastructure.[4]

This paper aims to highlight the importance of cybersecurity in protecting critical infrastructure. Given such an objective, one cannot fail to analyse the legislation which governs the status of owners and possessors of critical infrastructure facilities, installations and equipment, as well as operators of essential services (OES). Thus, the paper employs the dogmatic-legal method and the theoretical-legal method. The former makes it possible to analyse the existing legal provisions concerning protecting critical infrastructure that utilises cyberspace. In contrast, the theoretical-legal method is employed to assess the actions that should be taken to ensure critical infrastructure security, including its protection from threats.

THE SIGNIFICANCE OF CYBERSECURITY IN CRITICAL INFRASTRUCTURE PROTECTION

Regarding the objective scope, cybersecurity encompasses an increasingly broader spectrum relating to activities in cyberspace, spanning hardware, software, networks, systems, and human activity in that environment. Concerning the subjects

[1] M. Karpiuk, *Crisis Management vs. Cyber Threats*, "Sicurezza, Terrorismo e Societa" 2022, no. 2, p. 114.

[2] Article 2 (1a) of the Act of 21 June 2002 on the state of emergency (consolidated text, Journal of Laws 2017, item 1928).

[3] P. Milik, *Uwarunkowania globalne cyberbezpieczeństwa*, [in:] *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje*, eds. K. Chałubińska-Jentkiewicz, A. Brzostek, Warszawa 2021, p. 12.

[4] 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. 117.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

involved and advancing digitisation, cyber threats may affect individuals, communities, organisations, public entities, and even states. It is, therefore, reasonable to conceive of cybersecurity as a public good.[5] The lawmaker defines cybersecurity as the resilience of information systems against actions compromising the confidentiality, integrity, availability, and authenticity of the processed data or the related services such systems provide.[6]

According to the statutory definition, critical infrastructure means systems and their constituent, functionally related facilities, such as buildings, equipment, installations, and services that are key to the security of the state and its citizens, as well as serve to ensure the efficient functioning of public administration bodies, institutions, and businesses. Hence, critical infrastructure includes systems involved in: 1) supply of energy, energy raw materials, and fuels; 2) communications; 3) ICT networks; 4) finance; 5) food supply; 6) water supply; 7) health care; 8) transport; 9) rescue; 10) ensuring continuity of operation of public administration; 11) production, storage, keeping and use of chemical and radioactive substances, including pipelines of hazardous substances.[7] Although it employs fairly vague

[5] T. Zdzikot, *The Role of the State and Public Administration in the Cybersecurity System*, [in:] *The Role of Cybersecurity in the Public Sphere – the European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022, p. 40. Security is a domain of tremendous significance for the state (as a public institution), but it is also vital for society as a whole and individual citizens. Consequently, it should be considered a common good. See M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, "Zeszyty Naukowe KUL" 2018, no. 3, p. 15. As a common good, the security of the state may also be protected be means of declaring a state of emergency. See eadem, *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, "Roczniki Nauk Społecznych" 2013, vol. 3, p. 69. As a domain of security, cybersecurity qualifies as a common good as well.

[6] Article 2 (4) of the Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws 2023, item 913, as amended), hereinafter: ANCS. Concerning cybersecurity, see also D. Skoczylas, *Krajowy system cyberbezpieczeństwa*, Warszawa 2023; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3); K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, "Cybersecurity and Law" 2019, no. 1; C. Banasiński, M. Rojszczak (eds.), *Cyberbezpieczeństwo*, Warszawa 2020; A. Pieczywok, *The Use of Selected Social Concepts and Educational Programmes in Counteracting Cyberspace Threats*, "Cybersecurity and Law" 2019, no. 2; I. Hoffman, M. Karpiuk, *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex localis – Journal of Local Self-Government" 2022, vol. 20(3); J. Krawiec, *Cyberbezpieczeństwo. Podejście systemowe*, Warszawa 2019; J. Kostrubiec, *The Position of the Computer Security Incidents Response Teams in the National Cybersecurity System*, "Cybersecurity and Law" 2022, no. 2; W. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021; A. Pieczywok, *Cyberspace as a Source of Dehumanization of the Human Being*, "Cybersecurity and Law" 2023, no. 1; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019; C. Bravo, *Cyberbezpieczeństwo dla zaawansowanych*, Gliwice 2023; K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński (eds.), *Cybersecurity in Poland: Legal Aspects*, Cham 2022.

[7] Article 3 (2) of the Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws 2023, item 122), hereinafter: CMA.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

concepts, the definition above of critical infrastructure – in the Constitutional Tribunal's opinion – still contains commonly used terms and does not require a more detailed explanation in the provisions formulated solely in the Crisis Management Act. Indeed, the possibility of a complementary clarification of the definitions arises from the normative content of the entire act. The term comprises systems listed enumeratively. Critical infrastructure also includes the facilities and essential services within such systems.[8]

Referred to in the National Cybersecurity System Act, the sectors in which essential services are provided are essential to the state, economy and society, including energy, transport, banking and financial market infrastructure, health care, drinking water supply and distribution, and digital infrastructure.[9]

Pursuant to Article 3 (2) (a) CMA, critical European infrastructure encompasses systems and their functionally related facilities, including buildings, equipment and installations that are crucial for the security of the state and its citizens and ensure efficient functioning of public administration bodies, institutions and businesses concerning electricity, oil and natural gas, as well as road, rail, air, inland waterway, ocean, short-sea and port transportation, located in the territory of the Member States of the European Union, whose disruption or destruction would have a significant impact on at least two Member States.

In Article 3 (3) CMA, the lawmaker also defined critical infrastructure protection, which denotes all activities aimed at ensuring functionality, continuity of operations and integrity of critical infrastructure in order to prevent, mitigate and neutralise threats, risks or vulnerabilities, and to ensure their prompt restoration in the event of failures, attacks or other events disrupting their proper functioning. Protection of critical infrastructure is not only an ongoing but also a dynamic affair, as the perception of threats, the extent of available resources and protection capacity are subject to change. Critical infrastructure protection concerns various aspects of its functioning and integrates protection measures specific to different domains.[10]

The tasks within critical infrastructure protection are set out in Article 6 (1) CMA, according to which they include: 1) collection and processing of information on threats to critical infrastructure; 2) development and implementation of procedures in the event of a threat to critical infrastructure; 3) restoration of critical infrastructure; 4) cooperation between public administration and owners and owner-like possessors of facilities, installations or equipment of critical infrastructure concerning its protection.

[8] Judgment of the Constitutional Tribunal of 21 April 2009, K 50/07, Legalis no. 126072.

[9] Essential services are listed in the Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and disruptive effect thresholds of an incident in respect to the provision of essential services (Journal of Laws 2018, item 1806, as amended).

[10] M. Nowikowska, *Protection of Critical Infrastructure in Cyberspace*, [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022, p. 80.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

The Council of Ministers, as stipulated in Article 5b (1) CMA, adopts the National Programme for the Protection of Critical Infrastructure (hereinafter: the programme) by way of a resolution to create conditions to improve critical infrastructure security, particularly where it concerns: 1) preventing disruptions in the functioning of critical infrastructure; 2) preparation for contingencies that may adversely affect critical infrastructure; 3) responding to destruction or disruption of critical infrastructure; 4) restoring critical infrastructure. The conditions in which critical infrastructure security is improved are to be created by: 1) implementing the designated priorities and objectives of the programme; 2) ensuring conditions for enhanced protection and continuity of the functioning of critical infrastructure; 3) preparing for contingencies that may result from the disruption of or adversely affect the functioning of critical infrastructure; 4) preparing to respond to destruction or disruption of critical infrastructure; 5) creating conditions in which critical infrastructure may be restored; 6) compliance with the standards and requirements contained in the programme; 7) cooperative implementation of the programme.

Collaboration as part of the National Programme for the Protection of Critical Infrastructure consists of maintaining contact between the parties involved through conferences, seminars, discussion forums, preparation and participation in exercises and trainings, as well as exchange of information pertaining to: 1) identification of areas of action necessary to increase the degree of protection of critical infrastructure; 2) identified threats to critical infrastructure; 3) expected or observed increases in demand for services or products provided by critical infrastructure operators; 4) anticipated interruptions or disruptions in the supply of services or products provided by critical infrastructure operators; 5) supporting actions taken by critical infrastructure operators in the event of destruction or disrupted functioning of such infrastructure; 6) protection of critical infrastructure, functioning of internal protection mechanisms and crisis management; 7) preparation and updates of the programme.[11]

Article 6 (5) CMA imposes an obligation on owners as well as owner-like and dependent possessors of critical infrastructure facilities, installations or equipment to protect them, notably by preparing and implementing critical infrastructure protection plans − corresponding to the anticipated threats − as well as by maintaining their own backup systems that ensure security and sustained functioning of such infrastructure until it is fully restored. If they simultaneously happen to be OES, their critical infrastructure protection plans must incorporate documents concerning the cybersecurity of the information systems used to provide essential services.

Documents relating to the cybersecurity of the information systems that provide essential services include normative and operational files. The former include: 1) documents on the information security management system; 2) documents on

[11] § 7 of the Regulation of the Council of Ministers of 30 April 2010 on the National Programme for the Protection of Critical Infrastructure (Journal of Laws 2010, no. 83, item 541).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

the protection of the infrastructure utilised to provide an essential service, which contain the following: a) characteristics of the essential service and infrastructure, b) risk assessment for infrastructure facilities, c) assessment of the current state of infrastructure protection (risk management plan), d) description of technical safeguards of infrastructure facilities, e) principles according to which physical protection of infrastructure is organised and performed, f) data on specialised, armed security formation (internal security service and entrepreneur licensed to conduct business in personal and property protection, possessing firearms as a holder of a weapons permit, in line with Article 2 (7) of the Act of 22 August 1997 on the protection of persons and property, consolidated text, Journal of Laws 2021, item 1995, as amended), which protects the infrastructure, if such a formation exists; 3) documents on the management system to ensure continued provision of the essential service; 4) technical file on the information system utilised to provide the essential service; 5) documents specific to the essential service provided in a given sector or sub-sector. Operational documents consist of: 1) documents regarding the procedures and instructions arising from the normative documents; 2) a description of the mode of documenting the performance of the activities within the established procedures; 3) documents certifying each performance of a relevant procedure.[12]

Pursuant to Article 5 (1) and (2) ANCS, an OES is an entity whose organisational unit is located on the territory of the Republic of Poland and has been officially recognised as an OES by the competent cybersecurity authority. The competent cybersecurity authority issues a decision that an entity be recognised as OES if: 1) the entity provides an essential service; 2) the provision of that service relies on information systems; 3) an incident would have a significant disruptive effect on the provision of the essential service by that operator.

An OES plays a major role in ensuring cybersecurity at the national level, especially as it is an important element of the national cybersecurity system. Once an entity becomes an OES, it is subject to certain obligations, including protecting the information system used to provide such a service.[13]

Defined in Article 3 (1) CMA, a contingency is a situation which adversely affects the security of persons, extensive property or the environment, though it may also have its corollaries in cyberspace.[14] The threats resulting in a contingency are

[12] § 1–3 of the Regulation of the Council of Ministers of 16 October 2018 on documents regarding cybersecurity of the information system used for the provision of essential services (Journal of Laws 2018, item 2080).

[13] M. Karpiuk, *Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4, p. 166.

[14] As regards threats which result in contingencies, see M. Karpiuk, T. 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" 2020, vol. 29(1).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

likely to have a detrimental impact on the continued operation of critical infrastructure which uses ICT systems. The owners and possessors of critical infrastructure facilities, installations or equipment are obligated to protect them; this duty extends to the cyberspace in which such infrastructure operates.

Attention should also be drawn to protecting critical infrastructure when particular threats are in evidence, including those requiring a state of emergency. Major events in this regard include technical failures, whose aftermath poses a danger to the life or health of a large number of people, extensive property or the environment over a wide area, whereby the state of natural disaster has to be introduced.[15] The concept of a natural disaster implies that it is a global event affecting a large area of the natural environment.[16] Meanwhile, technical failures can be caused by cyberattacks. Facilities, equipment or installations involving cyberspace are exposed to several threats which undermine the efficiency of the ICT systems that provide vital services (for the state and society), which is why an adequate degree of cybersecurity must be ensured. Therefore, ICT systems within critical infrastructure must be resilient to cyber threats.

CONCLUSIONS

Strategic ICT systems are responsible for the stability of the state and its economy and must be adequately protected. They are also tremendously important for the citizens, which is why their reliability and security must be ensured. This should be a priority for those responsible for operating such systems, whether in the public or the private sector.[17]

The responsibility for the proper functioning of critical infrastructure rests with the state authorities and with the operators of the selected facilities, installations,

[15] Article 3 (1) (1) of the Act of 18 April 2002 on the state of natural disaster (consolidated text, Journal of Laws 2017, item 1897, as amended). See also M. Czuryk, *Zadania organów jednostek samorządu terytorialnego w stanie klęski żywiołowej*, "Zeszyty Naukowe AON" 2009, no. 3, p. 405. Counteracting threats in democratic states with the rule of law (including during a state of natural disaster) must not be an objective that the power strives to accomplish at the expense of other goods. See eadem, *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), p. 122. The actions of the public authority in a democratic state with the rule of law must inspire confidence among the citizens. See J. Kostrubiec, *Glosa do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 17 października 2017 r., V SA/Wa 2821/16*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), p. 219.

[16] Judgment of the Supreme Administrative Court of 11 March 2011, II GSK 347/10, Legalis no. 360767.

[17] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, pp. 89–90.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

equipment and services.[18] Such a broad scope of responsibility (regarding the actors involved) is because public entities are not the only ones to own or possess the facilities, equipment or installations that make up critical infrastructure. Their efficient functioning requires ICT systems, which must be adequately protected given the tasks they perform. Critical and major incidents threaten the operation of critical infrastructure, whose operators must therefore apply corresponding measures to counteract such incidents and, should they occur, to promptly eliminate their aftermath and prevent future events.

Threats to critical infrastructure may take multiple forms, and they should be broadly interpreted.[19] In an age when the state relies on ICT systems to function, they may be interfered with or disrupted through cyberattacks. Thus, if the state is to function properly, it is indispensable for critical infrastructure in the strategic sectors to be effectively protected. Effective protection of such infrastructure means safeguarding ICT systems against cyber threats.

REFERENCES

Literature

Banasiński C., Rojszczak M. (eds.), *Cyberbezpieczeństwo*, Warszawa 2020.

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

Bravo C., *Cyberbezpieczeństwo dla zaawansowanych*, Gliwice 2023.

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

Chałubińska-Jentkiewicz K., Radoniewicz F., Zieliński T. (eds.), *Cybersecurity in Poland: Legal Aspects*, Cham 2022.

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), **DOI: https://doi.org/10.17951/sil.2021.30.4.111-124**.

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

Czuryk M., *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, "Roczniki Nauk Społecznych" 2013, vol. 3.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3), **DOI: https://doi.org/10.17951/sil.2022.31.3.31-43**.

Czuryk M., *Zadania organów jednostek samorządu terytorialnego w stanie klęski żywiołowej*, "Zeszyty Naukowe AON" 2009, no. 3.

Dziomdziora W., *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021.

[18] M. Nowikowska, *op. cit.*, p. 80.

[19] M. Karpiuk, *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), p. 191.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

Hoffman I., Karpiuk M., *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex localis – Journal of Local Self-Government" 2022, vol. 20(3), **DOI: https://doi.org/10.4335/20.3.617-640(2022)**.

Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, "Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Crisis Management vs. Cyber Threats*, "Sicurezza, Terrorismo e Societa" 2022, no. 2.

Karpiuk M., *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), **DOI: https://doi.org/10.17951/sil.2019.28.1.185-194**.

Karpiuk M., *Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4, **DOI: https://doi.org/10.36128/priw.vi42.524**.

Karpiuk M., Włodek T., *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" 2020, vol. 29(1), **DOI: https://doi.org/10.17951/sil.2020.29.1.273-290**.

Kostrubiec J., *Glosa do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 17 października 2017 r., V SA/Wa 2821/16*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), **DOI: https://doi.org/10.17951/sil.2019.28.1.207-220**.

Kostrubiec J., *The Position of the Computer Security Incidents Response Teams in the National Cybersecurity System*, "Cybersecurity and Law" 2022, no. 2.

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)**.

Krawiec J., *Cyberbezpieczeństwo. Podejście systemowe*, Warszawa 2019.

Milik P., *Uwarunkowania globalne cyberbezpieczeństwa*, [in:] *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje*, eds. K. Chałubińska-Jentkiewicz, A. Brzostek, Warszawa 2021.

Nowikowska M., *Protection of Critical Infrastructure in Cyberspace*, [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Pieczywok A., *Cyberspace as a Source of Dehumanization of the Human Being*, "Cybersecurity and Law" 2023, no. 1.

Pieczywok A., *The Use of Selected Social Concepts and Educational Programmes in Counteracting Cyberspace Threats*, "Cybersecurity and Law" 2019, no. 2.

Skoczylas D., *Krajowy system cyberbezpieczeństwa*, Warszawa 2023.

Zdzikot T., *The Role of the State and Public Administration in the Cybersecurity System*, [in:] *The Role of Cybersecurity in the Public Sphere – the European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022.

Legal acts

Act of 18 April 2002 on the state of natural disaster (consolidated text, Journal of Laws 2017, item 1897, as amended).

Act of 21 June 2002 on the state of emergency (consolidated text, Journal of Laws 2017, item 1928).

Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws 2023, item 122).

Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws 2023, item 913, as amended).

Regulation of the Council of Ministers of 30 April 2010 on the National Programme for the Protection of Critical Infrastructure (Journal of Laws 2010, no. 83, item 541).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 02/02/2026 00:52:01

Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and disruptive effect thresholds of an incident in respect to the provision of essential services (Journal of Laws 2018, item 1806, as amended).
Regulation of the Council of Ministers of 16 October 2018 on documents regarding cybersecurity of the information system used for the provision of essential services (Journal of Laws 2018, item 2080).

Case law

Judgment of the Constitutional Tribunal of 21 April 2009, K 50/07, Legalis no. 126072.
Judgment of the Supreme Administrative Court of 11 March 2011, II GSK 347/10, Legalis no. 360767.

ABSTRAKT

Funkcjonowanie infrastruktury krytycznej jest uzależnione od systemów teleinformatycznych, które pozwalają na sprawne działanie urządzeń czy instalacji wchodzących w jej skład. Zagrożenia jej funkcjonowania mogą stanowić poważny problem dla państwa i społeczeństwa, gdyż obejmuje ona strategiczne sektory. Sektory te pokrywają się z usługami kluczowymi, za świadczenie których odpowiedzialni są operatorzy usług kluczowych. Ze względu na związek strategicznych systemów będących elementem infrastruktury krytycznej i jednocześnie odpowiadających za jej działanie z usługami kluczowymi, zapewnienie cyberbezpieczeństwa będzie wpływało również na ochronę tej infrastruktury. Należy podkreślić, że właściwa ochrona infrastruktury krytycznej może się odbywać przy zapewnieniu odporności na cyberzagrożenia wykorzystywanych przez nią systemów teleinformatycznych oraz przy wykorzystaniu współpracy sektora publicznego z sektorem prywatnym.

Słowa kluczowe: cyberbezpieczeństwo; cyberprzestrzeń; zarządzanie kryzysowe; infrastruktura krytyczna