Mirosław Karpiuk

Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level

Entities are recognized as operators of essential services by way of an administrative decision issued by a competent authority for ensuring cybersecurity. An operator of essential services is an entity providing a given essential service that relies on information systems, whereas an incident, seen as an event that has or might have a negative impact on cybersecurity, would have a substantial adverse effect on the provisions of an essential service by the said operator. An information system through which a given essential service is provided should be resilient to disruptions. If it serves the purpose of protecting services of strategic significance (including economic importance) to the state and society, it must be duly secured. Responsibilities in respect of security management within information systems are imposed on the operators of essential services.

Mirosław Karpiuk

associate professor in law
University of Warmia and Mazury in Olsztyn

ORCID – 0000-0001-7012-8999

e-mail: miroslaw.karpiuk@uwm.edu.pl

Key words:
cybersecurity, essential services,
information system, administrative decision

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

1. Introduction

The recognition of an entity as an operator of essential services has a significant influence on assuring cybersecurity at the national level, when such an operator is a part of the national cybersecurity system, constituting one of its vital links. As regards obtaining the status of an operator of essential services, relevant obligations are placed on the entity concerned, including tasks which consist of the protection of the information system used for providing such a service.

As regards performing activities which are seen as essential services, cybersecurity, defined as the ability of information systems to resist action that compromises the confidentiality, integrity, availability,

and authenticity of processed data or the related services offered by those information systems[1], is of great importance, not only for the operators themselves but also for the state and its security.

The notion of cybersecurity entails the protection of resources – data, information, digital content, the protection of information and communication (ICT) networks, hardware (meaning computers), and the protection of the transmission of content via networks, thus the communication process itself. The human factor should also be stressed here, including the protection of network and computer users. The key to activities posing all types of threats in cyberspace is to take advantage of vulnerabilities and errors in software development tools. There is no doubt that human actions are still a key part of the process[2].

Cybersecurity constitutes a specialized security system component which covers the protection of information systems against threats[3]. Cybersecurity is essential, not only due to the fulfilment of societal needs but also because of the uninterrupted functioning of public institutions[4]. It includes anticipating, counteracting, and combating threats, as well as eliminating the consequences of their occurrence[5]. The approach to threats must, first and foremost, be focused on prevention[6], which allows the mitigation of undesirable circumstances which might harm security, which also applies to such events as cyber-attacks.

Disruptions in cyberspace may have an adverse effect on society (not only in the sphere of performing professional duties in cyberspace, but also where it is used for communication purposes), and on the functioning of the state which is to ensure the quality of services of strategic importance. Given the need to properly secure such services, including their continuity and

1 Article 2(4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws of 2020, item 1369), further in the paper referred to as the "NCSA".

2 Katarzyna Chałubińska-Jentkiewicz, „Cyberbezpieczeństwo – zagadnienia definicyjne" *Cybersecurity and Law*, No. 2 (2019): 20.

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

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

5 Mirosław Karpiuk, „The Local Government's Position in the Polish Cybersecurity System" *Lex Localis – Journal of Local Self-Government*, No. 2 (2021): 612.

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

relevant reach (availability), it is becoming indispensable to undertake administrative measures aimed at their full protection. The recognition of an entity as an operator of essential services following an administrative procedure should be seen as one such measure.

The purpose of the paper is to describe the administrative procedure which is concluded with the issue of a decision on recognizing an entity as an operator of essential services. Such decisions, to a large extent, contribute to the increase of cybersecurity levels in such a vital sphere as the provision of essential services. A doctrinal legal research method was used in the paper. Binding legal regulations applicable to the procedure for recognizing an entity and an operator of essential services were analyzed using the method.

2. Categories of entities that may be recognized as operators of essential services

Pursuant to Article 5(1), an operator of essential services is an entity listed in Annex 1 to the NCSA, having an organizational unit in the territory of the Republic of Poland, in respect of which a competent authority for ensuring cybersecurity has issued a decision on recognizing the entity as an operator of essential services. Not all entities (including enterprises), even those operating in strategic sectors, will be able to obtain the status of operators of essential services.

As set out in Annex 1 to the NCSA, an entity which may be identified as an operator of essential services is: 1) in the energy industry[7] sector: a) mining: – an entity which conducts business activities in the scope of extracting natural gas or petroleum, lignite, bituminous coal or other fossils under a license, b) electricity: – an energy undertaking[8] holding a license to conduct

7 The issues of cybersecurity in the energy industry have been regulated by the NCSA which does not take into account the specific nature of the petroleum, natural gas and electricity sub-sectors. This does not favour the development of comprehensive and coherent solutions aimed at counteracting the risk of an incident. Individual Polish operators of essential services were additionally burdened by the obligation to implement a system which ensures cybersecurity, which is not always effective, Wojciech Konaszczuk, „Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution" *Studia Iuridica Lublinensia*, No. 4 (2021): 348.

8 An entity which conducts business activities in the scope of 1) production, processing, storage, transmission, the distribution of, or trade in, fuels or energy, and/or b) the transfer of carbon dioxide, and/or c) the transhipment of liquid fuels, Article 3(12) of the Energy Law of 10 April 1997 (consolidated text, Journal of Laws of 2022, item 1385, as amended), further in the paper referred to as the „EL".

business activities in the scope of generating electric power, or for the processing and storage of electric power, or in the scope of trade in electric power; – an energy undertaking holding a license to conduct business activities in the scope of electric power transmission (transmission system operator[9]); – an energy undertaking holding a license to conduct business activities in the scope of electric power distribution (distribution system operator[10]); – an entity which conducts business activities in the scope of providing system, quality and energy infrastructure services; c) heating: – an energy undertaking holding a license to conduct business activities in the scope of generating, trading in, transmitting, and distributing heating energy; d) petroleum: – an energy undertaking holding a license to conduct business activities in the scope of producing liquid fuels or transporting liquid fuels via a pipeline network; – an entity which conducts business activities in the scope of petroleum transmission; – an entity which conducts business activities in the scope of petroleum storage; – an entity holding a license to conduct business activities in the scope of petroleum transshipment; – an energy undertaking which conducts business activities in the scope of storing liquid fuels and an entity which conducts business activities in the scope of containerless underground storage of liquid fuels; – an energy undertaking which conducts business activities in the scope of liquid fuel transshipment, – an energy undertaking which conducts business activities in the scope of the trade in liquid fuels, or in the scope of the trade in liquid fuels with foreign entities, – entities which conduct business activities in the scope of the production of synthetic fuels; e) natural gas: – an energy undertaking which conducts business activities in the scope of producing gaseous fuels, – an energy undertaking which holds a license to conduct business activities in the scope of transporting gaseous fuels, and a license to conduct business activities in the scope of the trade in natural gas with foreign entities, or to conduct business activities in the scope

9 An energy undertaking that deals with the transmission of gaseous fuels or electricity, responsible for network traffic within the gas transmission system, or electric power transmission system, current and long-term security of the operation of the system, operation, maintenance, repairs, and necessary extension of the transmission network, including connections with other gas systems or other electrical power systems, Article 3(24) of the EL.

10 An energy undertaking which deals with the distribution of gaseous fuels or electric power, responsible for network traffic within the gas distribution system, or electric power distribution system, the current and long-term security of the operation of the system, operation, maintenance, repairs, and necessary extension of the distribution network, including connections with other gas systems or other electricity power systems, Article 3(25) of the EL.

of the trade in gaseous fuels, – an energy undertaking whom the President of the Energy Regulatory Office has assigned the functions of a gas transmission system operator, gas distribution system operator, operator of a gaseous fuel storage[11] system, gas liquefaction system operator[12]; f) energy sector supplies and services: – entities which conduct business activities in the scope of supplying systems, machines, devices, materials, raw materials and providing services for the energy sector, g) supervised and subordinate units: – organizational units subordinate to, or supervised by, the minister competent for energy, organizational units subordinate to, or supervised by, the minister competent for fossil deposits management; 2) in the transport industry sectors: air transport: – air carrier[13], – airport manager[14], – undertakings holding a license to provide ground handling services for air carriers and other aircraft users, in respect of one or more of the categories of ground handling services, and an enterprise being a regulated agent in respect of cargo and mail, performing security checks for air carriers; – an air navigation service provider, b) rail transport: – rail infrastructure manager[15], excluding infrastructure managers responsible for closed infrastructure, private infrastructure or narrow-gauge infrastructure; – railway undertakings[16] whose activities are subject

11 An energy undertaking which deals with the storage of gaseous fuels, responsible for the operation of storage facilities, Article 3(26) of the EL.

12 An energy undertaking which deals with the liquefaction of natural gas, imports, unloading or regasification of liquefied natural gas, responsible for the operation of such gas facilities, Article 3(27) of the EL.

13 An air transport undertaking holding a valid operating license or equivalent, Article 3(4) of Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ EU of 2008 L 97, p. 72).

14 An entity which has been entered as an operator in the register of civil airports, Article 2(7) of the Aviation Law of 3 July 2002 (consolidated text, Journal of Laws of 2022, item 1235).

15 An entity responsible for managing railway infrastructure, its operation, maintenance, renovation or participating in the development of the infrastructure, and where new infrastructure is built, as an entity which participates in construction works as a project owner, Article 4(7) of the Rail Transport Act of 28 March 2003 (consolidated text, Journal of Laws of 2021, item 1984, as amended), further referred to as the "RTA".

16 An enterprise authorized to perform rail transport services, including enterprises performing only traction services, under a license and a single safety certificate, or an enterprise authorized to perform rail transport services under a safety certificate, Article 4(9) of the RTA.

to licensing or operators of service facilities, if such enterprises concurrently have the function of a railway undertaking, c) water transport: – shipowners in maritime passenger and freight transport, – the owner of a ship or a person who has received a legal title to hold a ship in their own name (shipowner)[17], port authority[18], – an entity providing support activities to maritime transport on the site of ports, – Vessel Traffic Service (a body supporting the head of maritime authority, appointed to monitor vessel traffic and forward information, forming part of the SafeSeaNet National System[19]), d) road transport: – The General Directorate of National Roads and Highways, Province Board, District Board, Commune Head (Mayor), Metropolitan Union Board, depending on the category of a given public road[20], – an entity implementing smart transport systems; 3) in the banking and financial market infrastructure industry; – credit institution, – a national bank[21], a branch of a foreign bank[22], a branch of a credit institution, – cooperative savings and credit union, – an operator of a regulated market, – a legal person that interposes themselves between the counterparties to the contracts traded on one

17 Article 5(2) of the Inland Navigation Act of 21 December 2000 (consolidated text, Journal of Laws of 2022, item 1097).

18 An entity appointed to manage a port or a sea marina, Article 2(6) of the Act of 20 December 1996 on ports and sea marinas (consolidated text, Journal of Laws of 2022, item 1624).

19 To ensure the exchange of information about vessels or events which constitute a potential threat to navigation or safety at sea, the security of people or the maritime environment, the impact of which might extend to the Polish sea area or the sea areas of other European Union Member States, and the monitoring of vessel traffic, including the management of or supervision over vessel traffic, the National Vessel Traffic and Information System (National SafeSeaNet System) shall be established - Article 91 of the Act of 18 August on Maritime Security (consolidated text, Journal of Laws of 2022, item 515, as amended).

20 See Article 19 of the Public Roads Act of 21 March 1985 (consolidated text, Journal of Laws of 2021, item 1376, as amended).

21 A bank having its registered office in the territory of Poland, Article 4(1) (1) of the Act of 29 August 1997 − the Banking Law (consolidated text Journal of Laws of 2021, item 2439, as amended), further in the paper referred to as the „BL".

22 An organizational unit of a foreign bank performing all or some activities on its behalf under an authorization granted to the bank, whereas all organizational units of a given foreign bank, meeting the above conditions, and established on the territory of Poland, are deemed to form a single branch, Article 4(1)(20) of the BL.

or more financial markets, becoming the buyer to every seller and the seller to every buyer[23] with its registered office in the territory of Poland, – a joint-stock company being a subsidiary of Krajowy Depozyt Papierów Wartościowych S.A. (the Central Securities Depository of Poland)[24], 4) in the healthcare industry: – healthcare entity, – an entity subordinate to the minister competent for healthcare, responsible for information systems in healthcare, – the National Health Fund, – a healthcare entity in which a hospital pharmacy department or a hospital pharmacy operates, – an enterprise which conducts business activities involving the wholesale of pharmaceuticals, – an enterprise or entity which conducts business activities in a European Union Member State, a Member State of the European Free Trade Association (EFTA), a party to the agreement on the European Economic Area which has obtained marketing authorization for a medicinal product, an importer or manufacturer of a medicinal product or an active substance, – a parallel importer, an entity holding a permit to conduct activities in respect of importing medicinal products meeting specified conditions from European Union Member States or Member States of the European Free Trade Association (EFTA), – an active substance distributor, – an enterprise conducting business activities in the form of a general-access pharmacy, 5) in the drinking water supply and distribution industry: – a water-supply and sewage enterprise[25]; 6) in the digital infrastructure industry: – an entity providing DNS (Domain Name System) services, – an entity running an Internet exchange point (IXP) which allows inter-system connections between more than two independent autonomous systems, mainly to facilitate Internet traffic exchange, – an entity managing the Internet names register as part of a top level domain (TLD).

Operators of essential services are burdened with substantial responsibility for ensuring the cybersecurity of their operations and infrastructure[26].

23 See Article 2(1) of Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012on OTC derivatives, central counterparties, and trade repositories (OJ EU of 2012, L 201, p. 1).

24 See Article 48(7) of the Act of 29 July 2005 on the Trade in Financial Instruments (consolidated text, Journal of Laws of 2022, item 1500, as amended).

25 An enterprise, if it conducts business activities in the scope of collective water supply or sewage collection and municipal organizational units without legal personality which conducts such type of activities, Article 2(4) of the Act of 7 June 2001 on collective water supply and sewage collection (consolidated text, Journal of Laws of 2020, item 2028, as amended).

26 Aneta Chodakowska, Sławomira Kańduła, Joanna Przybylska, „Cybersecurity in the Local Government Sector in Poland: More Work

For that reason, a public administration entity that issues a decision on recognizing an entity as the operator must consider the effects of events that might have an adverse effect on the resilience of information systems that are used for the provision of essential services, and the need to impose specified obligations of a protective nature.

3. The procedure for recognizing an entity as an operator of essential services

A competent authority for ensuring cybersecurity issues a decision on recognizing an entity as an operator of essential services and handles proceedings in this matter. The list of competent authorities for ensuring cybersecurity is set out in Article 41 of the NCSA. It includes ministers competent for a given industry and the Polish Financial Supervision Authority for the banking and financial market infrastructure industries.

As per Article 5(2) of the NCSA a competent authority for ensuring cybersecurity issues a decision on recognizing an entity as an operator of essential services if 1) the entity concerned provides an essential service; 2) the provision of such service relies on information systems; 3) an incident is likely to cause a substantial disruption to the operator's provision of the essential service[27]. All the above conditions must be met jointly for a public administration body to be able to issue a decision on recognizing an entity as an operator of essential services. The entity concerned, as a party to administrative proceedings, must provide an essential service, which is a service defined in Article 2(16) of the NCSA, thus having a fundamental significance for the maintenance of critical societal or economic activities entered in the list of essential services. The provision of the service must rely on information systems, as defined in Article 2(14) of the NCSA, as information and communication systems, together with electronic data that are processed therein. In addition, an incident might have a substantial disruptive effect on the

Needs to be Done" *Lex Localis – Journal of Local Self-Government*, No. 1 (2022): 167. The operators of essential services are a key component of the national cybersecurity system, Jarosław Kostrubiec, „Cybersecurity System in Poland. Selected Legal Issues", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 10.

27 Article 5(2) of the NCSA is a legal norm governing power. For detailed information about legal norms governing responsibilities and powers, see Mirosław Karpiuk, Tomasz Włodek, "Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)" *Studia Iuridica Lublinensia*, No. 1 (2020): 283.

provision of a given essential service. A given incident is deemed to be a material incident if at least one of the conditions has been met: 1) a service provided by electronic means has been unavailable for over 5 000 000 user-hours (a user-hour refers to the number of users in the European Union affected by the incident for sixty minutes); 2) an incident has resulted in the loss of integrity, authenticity, or confidentiality of stored, transmitted or processed data, or related services offered by, or accessible via, network and information systems of a digital service provider, which has affected over 100 000 users across the European Union; 3) an incident has posed a threat to public security or a risk of the loss of life[28]. The definition of a material incident may prove helpful for decoding a significantly disruptive effect. Yet, they are not legally equivalent notions, and authority cannot automatically assume that a significant disruptive effect on the provision of an essential service occurs only in the event of a material incident. The potential range of the disruptive effect in cyberspace needs to be analyzed each time individually, notwithstanding the nature of the incident. On that basis, the probability of the disruptive effect for a given operator must be assessed. The materiality of the disruptive effect on the provision of an essential service is specified on other grounds, as stated in Article 5(3) of the NCSA, based on materiality thresholds of the disruptive effect.

The materiality threshold of a disruptive effect of an incident on the provision of an essential service is assessed by taking into account the following criteria: 1) the number of users relying on an essential service provided by a given entity; 2) the dependence of other sectors on the service provided by the entity in question; 3) the impact which a given incident might have on economic and societal activities and public security, in terms of its scale and duration; 4) the market share of a given entity providing an essential service; 5) the geographical reach, related to the area which might be affected by a given incident; 6) an entity's ability to maintain a sufficient level of essential services, taking into account alternative means of service provision; 7) other factors characteristic of a given sector[29]. Not all these criteria will refer

28 Article 4(1) of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ EU of 2018, L 26, p. 48).

29 Annex to the Regulation of the Council Ministers of 11 September 2018 on the list of essential services and materiality thresholds of the disruptive effect of incidents on the provision of essential services (Journal of Laws of 2018, item 1806).

to essential services provided in various industries and sectors, and if they do, the criteria might apply in various degrees.

Under Article 5(4), legislators have imposed on public administration authorities the obligation to perform additional actions if the activities of the entity providing an essential service go beyond the territory of Poland and are conducted within the European Union. Where an entity concerned provides an essential service in other European Union Member States, the competent authority for ensuring cybersecurity, during an administrative procedure and via a Single Point of Contact responsible for cybersecurity, holds consultations with relevant states to investigate whether the entity has been considered as an operator of essential services in these states. The Minister competent for computerization manages the Single Point of Contact responsible for cybersecurity, whose tasks include, *inter alia*, coordinating cooperation between competent authorities for cybersecurity and public authorities in Poland with relevant authorities in the other EU Member States. The above responsibility has been set out in Article 48(5) of the NCSA. While conducting administrative proceedings, the competent authority for cybersecurity uses legal assistance, as it does not have the powers which would allow it to request information from a relevant authority in each Member State to investigate whether a given entity providing an essential service, being a party to the proceedings, has been identified as an operator of essential services in the state concerned.

Administrative proceedings are instituted at the request of a party or *ex officio*. The NCSA does not set out the form of instituting proceedings for recognizing an entity as an operator of essential services. Therefore, both forms mentioned above are permissible. It can be assumed that, as a rule, it is the competent authority for cybersecurity that institutes the proceedings *ex officio*, because the concluding decision involves certain obligations to be placed on the party to the proceedings, while such an entity does not have any interest in such obligations and would not apply to the authority for instituting administrative proceedings, as a result of which an entity providing an essential service may obtain the status of an operator of essential services which involves several additional obligations related to ensuring cybersecurity.

A public administration authority is obliged to collect and examine the entire evidence exhaustively, and it may change, supplement, or repeal its decisions to examine evidence at any stage of the proceedings[30]. The authority

30 Article 77(1-2) of the Act of 14 June 1960 – Code of Civil Procedure (consolidated text, Journal of Laws of 2021, item 735, as amended), further in the paper referred to as the „CAP".

has the legal obligation to collect evidence during administrative proceedings and to take all the necessary steps to clarify the matter in question[31].

The competent authority for ensuring cybersecurity, as the authority conducting administrative proceedings, should examine all circumstances which are relevant in each matter. The authority should analyze the evidence collected in the matter, and an investigation should be conducted where necessary.

Any findings as to the facts identified by the authority should refer to all elements which are conditions for considering a given entity as an operator of essential services. The competent authority for cybersecurity may not limit itself to merely pointing to the evidence collected in the matters and quoting applicable legal regulations. It must also identify and demonstrate a relationship between individual conditions, particularly the link between the provision of a given service and its reliance on the functioning of an information system, and/or analyze the significance of a disruptive effect[32].

An entity is recognized as an operator of essential services by an administrative decision, whereas the NCSA does not specify its parts. Therefore, such a decision must be compliant with the requirements provided for in Article 107 § 1 of the CAP and must include: 1) the name of the public administration body; 2) the date of issue; 3) the name of the party or parties; 4) the legal basis; 5) the decision; 6) factual and legal grounds; 7) instructions as to the right to appeal against the decision and the applicable procedure, the right to waive appeal entitlement, and the effects of such waivers; 8) signature, full name and the official position of the authority's employee authorized to issue the decision. An administrative decision, as a procedural action which concludes proceedings and specifies a party's obligations, should satisfy any formal requirements provided for in procedural law.[33] If any of the elements are missing, the decision is defective, whereas not all defects result in eliminating such a decision from the legal order. Minor defects of an administrative decision will not result in its revocation or invalidity.

31 Monika Sadowska, „Komentarz do art. 77", [in:] *Kodeks postępowania administracyjnego. Komentarz do art. 61-126*, ed. Mirosław Karpiuk, Przemysław Krzykowski, Agnieszka Skóra (Olsztyn: UWM, 2020), 142.

32 Dorota Lebowa, „Procedure for the Identification of an Operator of Essential Services under the Act on the National Cybersecurity System", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec (Maribor: Lex Localis Press, 2022), 108.

33 Monika Sadowska, „Komentarz do art. 107", [in:] *Kodeks postępowania administracyjnego. Komentarz do art. 61-126*, ed. Mirosław Karpiuk, Przemysław Krzykowski, Agnieszka Skóra (Olsztyn: UWM, 2020), 264.

The competent authority for ensuring cybersecurity also decides about the annulment of the status of the operator of essential services by way of an administrative decision. Under Article 5(6) of the NCSA, in respect of an entity which no longer meets the statutory conditions, the competent authority for ensuring cybersecurity issues a decision on the expiration of a decision to recognize an entity as an operator of essential services. If a given entity that provides an essential service no longer meets the conditions provided for in Article 5(1)-(2) of the NCSA, the competent authority for ensuring cybersecurity is obliged to issue a decision on the expiration of the original decision on recognizing the entity as an operator of essential services. The decision does not expire by law, but it is necessary to institute administrative proceedings and to find in their course that the party concerned no longer meets the statutory conditions which are required to be awarded the status of an operator of essential services and to issue a decision to repeal the original decision on recognizing an entity as an operator of essential services.

The decision on recognizing an entity as an operator of essential services and the decision on the expiration of such a decision are immediately enforceable. Such a rule is laid down in Article 5(7) of the NCSA. This solution seems indisputable since the provision of essential services has excellent significance for ensuring security in cyberspace, even more so since such services are of a strategic nature from the state's perspective. As regards the expiration decision, the immediate enforceability rule protects a given party against the need to fulfill additional obligations where statutory conditions are no longer being met.

4. Conclusion

Cybersecurity is of great importance in a digital state, and the outcomes of actions affecting this type of security resonate not only in the public sphere but also in the social sphere. Therefore, the state's response to cyber--attacks must be prompt and strong and include a search for state-of-the-art protection mechanisms. In response to the increasing number of threats in cyberspace, the legislators have found that it is necessary to provide appropriate legal regulations, allowing a proper diagnosis of an adequate response to cyber-attacks[34].

One of the primary tasks of the state is to ensure digital security. The functioning of a digital society is based on information systems which are prone to disruptions affecting their operation. The threats which cover the informational side of social existence give rise to increasingly serious consequences, and cyber-attacks may also be used as a tool for economic and political

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

pressure[35]. Information systems should operate uninterruptedly, they must be resilient to actions that are likely to result in the deterioration of quality or disruptions of tasks being performed[36]. Such systems also serve the provision of essential services whose significance to the state and society in the digital era should not be underestimated, as they have the potential to ensure not only stability but also development. Essential services are of key importance to social and economic activities, determining them to a large extent, and are vital to maintaining the security of the critical infrastructure. Due to their significance, it is necessary to ensure their protection which is provided through, *inter alia*, the award of the status of an operator of essential services to an entity that renders such services, which involves additional security-related obligations. This security requires, for example, the implementation of technological solutions ensuring not only the continuity of essential services but also their availability and quality.

Bibliography

Chałubińska-Jentkiewicz Katarzyna, „Cyberbezpieczeństwo – zagadnienia definicyjne" *Cybersecurity and Law*, No. 2 (2019): 7-23.

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

Czuryk Małgorzata, „Activities of the Local Government During a State of Natural Disaster" *Studia Iuridica Lublinensia*, No. 4 (2021): 111-124.

Czuryk Małgorzata, „Supporting the Development of Telecommunications Services and Networks Through Local and Regional Government Bodies, and Cybersecurity" *Cybersecurity and Law*, No. 2 (2019): 39-50.

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

Kaczmarek Krzysztof, „Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii" *Cybersecurity and Law*, No. 1 (2019): 143-157.

35 Krzysztof Kaczmarek, „Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii" *Cybersecurity and Law*, No. 1 (2019): 145.

36 Istvan Hoffman, Mirosław Karpiuk, „E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues" *Lex Localis – Journal of Local Self-Government*, No. 3 (2022): 629.

Karpiuk Mirosław, „The Local Government's Position in the Polish Cybersecurity System" *Lex Localis – Journal of Local Self-Government*, No. 2 (2021): 609-620.

Karpiuk Mirosław, „The Organisation of the National System of Cybersecurity: Selected Issues" *Studia Iuridica Lublinensia*, No. 2 (2021): 233-244.

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

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

Konaszczuk Wojciech, „Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution" *Studia Iuridica Lublinensia*, No. 4 (2021): 333-351.

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

Lebowa Dorota, „Procedure for the Identification of an Operator of Essential Services under the Act on the National Cybersecurity System", [in:] *The Public Dimension of Cybersecurity*, ed. Mirosław Karpiuk, Jarosław Kostrubiec. 101-110. Maribor: Lex Localis Press, 2022.

Madziar Ilona, Karolina Szelągowska, „Komentarz do art. 107", [in:] *Kodeks postępowania administracyjnego. Komentarz do art. 61-126*, ed. Mirosław Karpiuk, Przemysław Krzykowski, Agnieszka Skóra. 263-305. Olsztyn: UWM, 2020.

Sadowska Monika, „Komentarz do art. 77", [in:] *Kodeks postępowania administracyjnego. Komentarz do art. 61-126*, ed. Mirosław Karpiuk, Przemysław Krzykowski, Agnieszka Skóra. 142-145. Olsztyn: UWM, 2020.