European Research Studies Journal
Volume XXVIII, Issue 4, 2025

pp. 191-205

The Status of Essential Service Operators in the National Cybersecurity System in Poland: Considerations in the Context of European Union Regulations

Submitted 01/09/25, 1st revision 20/09/25, 2nd revision 18/10/25, accepted 10/11/25

Elżbieta Kurzępa-Piękoś[1], Sylwia Dziedzic[2], Michał Kościółek[3]

Abstract:

Purpose: *The aim of this publication is to define the role of essential service operators in the cybersecurity system in Poland, as entities essential to the proper functioning of the economy and society and jointly responsible for ensuring national security and the stability of the state. Furthermore, the publication aims to present a description of the legal status of these entities and the basic tasks arising from the provisions of the Act of July 5, 2018, on the National Cybersecurity System. Reference is also made to European Union regulations, which led to the identification of these entities under national law.*
Design/Methodology/Approach: *The research method adopted in this publication is a legal-dogmatic method and a legal-comparative method.*
Findings: *After analyzing current national and EU regulations, the article highlights changes in cybersecurity policy resulting from the entry into force of the new European Union directive – NIS 2. Furthermore, the article identifies the directions of changes in Polish legislation regarding the classification of essential entities that will soon replace essential service operators, which in turn is caused by the need to implement the NIS 2 directive. It was confirmed that the regulations adopted regarding the operation of these entities are consistent with European Union law.*
Practical implication: *Defining the directions of changes in the classification of essential entities that will replace essential service operators and identifying the related potential organizational and financial challenges for many businesses may constitute an important voice in the public debate regarding the proper functioning of the cybersecurity system in Poland and the costs generated by the potential adaptation of this security sphere to EU requirements.*
Originality/Value: *The effects of actual changes in the national cybersecurity system, caused by the need to implement the NIS2 Directive, constitute an interesting research area, and the role of essential service operators in the cybersecurity system is relatively rarely addressed in the literature. The conclusions presented in this area may constitute a valuable contribution to the researched issue and provide potential guidance in the further process of normative shaping of the cybersecurity system in Poland.*

[1]*Rzeszow University of Technology, Poland, ORCID: 0000-0003-0032-8607, e-mail: e_kurzepa@prz.edu.pl;*
[2]*The same as in 1, ORCID: 0000-0002-3852-5609, e-mail: dziedzic@prz.edu.pl;*
[3]*The same as in 1, ORCID: 0000-0002-4059-9244, e-mail: mkos@prz.edu.pl;*

Keywords: *Essential entities, NIS Directive 2, NIS Directive 1.*

JEL codes: *J28, K23, L38.*

Paper type: *Research article.*

1. Introduction

Cybersecurity is currently a key element of national security. As recent events have shown, it has become the focus of attention not only on state authorities in the context of developing regulations to protect it, but also on external entities interested in taking hostile actions against individual entities in this sphere (Górka, 2018).

Often, these entities will be of strategic importance to the state, including those in the energy, transportation, and healthcare sectors. The development of ICT technologies, in addition to its undoubtedly positive aspects, also influences the occurence of negative phenomena in cyberspace, such as cybercrime, cyberconflicts, cyberwarfare (information warfare), and cyberwar (Mąkosa, 2021).

It is increasingly being noted that global threats related to cybercrime and cyberterrorism are being classified as situations that threaten the stability and security of the state (Woszek, 2022). The literature on the subject argues that cyber threats have weakened traditional forms of political power, and in response, nation states are increasingly seeking to control processes occurring in cyberspace (Vacca, 2011).

Growing threats aimed at institutions using IT systems in their operations, as well as emerging EU requirements regarding the need to harmonize the rules for ensuring security in cyberspace, led to the adoption in Poland of the Act of 5 July 2018 on the national cybersecurity system, which sets essential service operators in a special place among the entities creating the cybersecurity system in Poland.

According to the justification for this bill: "The ever-increasing impact of ICT on the socio-economic development of European Union Member States and the increase in their use mean that the products and services offered are now increasingly dependent on ensuring cybersecurity. The extensive architecture of ICT systems, including operations on large data resources, serves the development of communications, trade, and transport, and constitutes the basis for the functioning of key digital services and services provided by public administration.

Unfortunately, the possibilities offered by modern digital technologies are also used to engage in unfair competition practices, interrupt the continuity of selected services (whether for hooligan purposes or to weaken the competitive position of a given entity), commit crimes using the Internet, or conduct terrorist activities. Therefore, the commencement of work related to the comprehensive regulation of the national cybersecurity system stems, on the one hand, from the need to ensure a systemic approach to the national cybersecurity system in the face of constantly growing and dynamically changing cybersecurity threats to the functioning of the state, economy, and society, and, on the other hand, from the need to implement Directive 2016/1148 into the Polish legal system" (Justification of the draft, 2018).

The explanatory memorandum to the bill further notes that it aims to define the organization and operation of the national cybersecurity system, the manner of exercising supervision and control over the application of the provisions of the act, and the scope and procedure for establishing the Cybersecurity Strategy of the Republic of Poland. It should be noted that increasing cybersecurity at the national level, including in the area of key and digital services and critical infrastructure, is one of the assumptions of the "Cybersecurity Strategy of the Republic of Poland for 2019-2024" (Resolution No 125, 2019).

The thesis of this publication is that essential service operators play an important role in the national cybersecurity system, ensuring the continuity of services of strategic importance to the state. The legal framework for their operation in Poland aligns with the standards set by European Union regulations.

The research method used to support this thesis is a legal-dogmatic approach, based on analysis of available literature, journalism, and applicable normative acts. A comparative legal approach was also employed to compare regulations adopted in the Polish legal system and solutions contained in European Union law regarding the status and role of essential service operators in cybersecurity policy.

2. Literature Review

It should be noted that detailed issues regarding the cybersecurity system in Poland and its dependence on European Union legal standards, including the classification of entities constituting the cybersecurity system and changes in this regard related to the implementation of the NIS 2 Directive, are relatively rarely addressed in the literature and occasionally become the subject of broader discussion.

Definitions of essential service operators and a catalog of their legal obligations are included in the provisions of the Act of 5 July 2018 on the National Cybersecurity System and are a result of the implementation of the so-called NIS 1 Directive. An in-depth analysis and interpretation of these issues was undertaken primarily in the commentary on the aforementioned Act of 5 July 2018 on the National Cybersecurity System, edited by Czaplicki (2019).

However, it should be noted that this publication, which comprehensively addresses the provisions of the Act of 5 July 2018 and presents them in the context of EU solutions, concerns the legal status prior to the implementation of the NIS 2 Directive. Furthermore, issues related to the structure of the national cybersecurity system and the role of essential service operators as an important element in this system have been addressed incidentally in scientific articles on cybersecurity, without in-depth analysis of these detailed issues (Oleksiewicz, 2020; Kosior, 2019; Kurzępa-Piekoś, 2024).

It should be noted that the discussion regarding the assumptions of the so-called NIS 2 Directive and the resulting changes in the nomenclature of entities constituting the cybersecurity system, as well as changes in the scope of these entities' responsibilities, is currently taking place in journalistic articles online (Wrzosek 2021; Czekil, 2025; BSJP, 2020).

The discussion primarily focuses on the draft amendments to the Act of 5 July 2018 on the National Cybersecurity System, including the new method of classifying entities (Government Legislative Center, 2025). A more in-depth scientific discussion in this area is likely to begin after the new national regulations implementing the NIS 2 Directive enter into force.

3. Research Methodology

The thesis adopted in this publication is that essential service operators play an important role in the national cybersecurity system, as entities ensuring the continuity of services of strategic importance to the state, and the legal framework for their operation in Poland is consistent with standards set by European Union regulations.

The research method used to support this thesis is a legal-dogmatic method, based on an analysis of available literature on the subject, journalistic writings, and applicable normative acts. It should be noted that the legal-dogmatic method is a research approach that focuses on the analysis and interpretation of legal provisions and court rulings. Its goal is to establish the principles and rules that govern the legal system.

This method is based on logical reasoning and a systematic approach to legal analysis. A comparative legal method was also employed to compare regulations adopted in the Polish legal system and solutions contained in European Union legal acts regarding the status and role of essential service operators in cybersecurity policy.

The method used was also necessary to determine the origins of the entities in question – key service operators – in the Polish legal system and the pattern of regulations adopted in Poland in this regard.

3.1 Current Solutions for the Functioning of Essential Service Operators - National and EU Context

As indicated in the above considerations, the direct reason for the adoption of the Act of 5 July 2018 on the National Cybersecurity System, which is the first legal act in Poland comprehensively regulating this sphere of public life, was the need to implement 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 (hereinafter referred to as NIS) (Directive - 2016/1148).

The legal basis for the NIS Directive was Article 114 of the Treaty on the Functioning of the European Union, relating to the internal market. The primary goal of the directive was to create a level playing field among European Union Member States by establishing the requirement to have a competent authority for cybersecurity, as well as the ability to respond to technical incidents at the national level (Oleksiewicz 2020 a).

It required all European Union Member States to ensure a minimum level of national cybersecurity capabilities by establishing competent authorities and a single point of contact for cybersecurity, establishing computer emergency response teams (CSIRTs), and adopting national strategies (Kosior, 2020).

The NIS Directive introduced two categories of entities – addressees of numerous obligations that play important roles in the cybersecurity system: operators of essential services and digital service providers. According to Article 4(4) of the Directive, "operator of essential services" means a public or private entity of one of the types referred to in Annex II, meeting the criteria set out in Article 5(2).

The criteria for identifying operators of essential services, referred to in Article 4(4), are as follows:

a) The entity provides a service that is essential to maintain critical social or economic activities;
b) The provision of this service depends on networks and information systems; and
c) The incident would have a significant disruptive effect on the provision of this service.

According to Annex II of the Directive, operators of essential services include, among others, energy companies, oil pipeline operators, gas supply companies, airlines, railway companies, inland, maritime, and coastal passenger and freight water transport operators, credit institutions, healthcare facilities, including hospitals and private clinics, suppliers and distributors of water intended for human consumption (Kurzępa-Piękoś, 2024).

It should be noted that the NIS Directive was repealed by another EU legal act – Directive (EU) 2022/2555 of the European Parliament and of the Council concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, adopted on 14 December 2022 (Directive 2022/2555). It established new standards for cybersecurity and the identification of entities creating national cybersecurity systems.

Compared to the previously applicable NIS Directive from 2016, the new NIS 2 Directive has generated the need to introduce numerous changes at the level of national legislation, including the classification of entities creating cybersecurity systems. However, for now, solutions stemming from the regulations contained in the NIS Directive are still formally in force in Poland.

Poland is expected to implement the changes resulting from the adoption of the NIS 2 Directive in the second quarter of 2025, although the initial deadline for implementing the EU guidelines was set for October 17, 2024 (Ministry of Infrastructure, 2025). Draft amendments related to the implementation of the NIS 2 Directive, which are currently controversial, will be analyzed later in this publication.

Moving on to the still-applicable national regulations establishing the cybersecurity system in Poland, it should be noted that the legislature has, of course, adapted national solutions to the standards set out in the now-repealed NIS Directive (Wąsowski, 2021).

A closed list of entities within the national cybersecurity system is contained in Article 4 of the Act on the National Cybersecurity System and includes 20 categories of various institutions. At the top of this list, in Article 4, points 1 and 2, the legislature, implementing the guidelines of the NIS Directive, lists operators of essential services and digital service providers.

The literature on the subject points out that the broad catalogue of entities of the national cybersecurity system, going beyond the scope necessary to implement the directive, can be divided into three groups: 1) system administration: authorities and other administrative entities and the relations between them; 2) participants: operators of essential services and digital service providers, as well as public entities as addressees of the obligations referred to in section 5; 3) entities supporting participants: entities providing cybersecurity services and accredited assessment bodies (Czplicki, 2019).

Operators of essential services referred to in Art. 4 point 1 are entities with organizational units in the territory of the Republic of Poland, for which the authority competent for cybersecurity has issued a decision recognizing them as essential service operators. The sectors (energy, transport, banking and financial market infrastructure, healthcare, drinking water supply and distribution, digital infrastructure), subsectors and types of entities are specified in Annex 1 to the Act.

The authority competent for cybersecurity issues a decision recognizing an entity as an essential service operator if: 1) the entity provides an essential service; 2) the provision of this service depends on information systems; 3) an incident would have a significant disruptive effect on the provision of an essential service by this operator (Art. 5 sec. 2).

The category of essential service operators includes, for example, entities conducting business activities in the field of natural gas extraction on the basis of a license; an energy company holding a license to conduct business activities in the field of electricity generation; entities conducting business activities in the field of crude oil transshipment; an airport operator; a railway carrier whose activities are subject to licensing; shipowner; medical entity; national bank; water and sewage company; an entity managing the registration of Internet domain names under the top-level domain (Czyżak, 2023).

In light of current regulatory solutions, the most important responsibilities of essential service operators include:

1) risk management (including risk assessment);
2) implementing appropriate and proportionate technical and organizational measures to the assessed risk (including maintenance and secure operation of the information system; physical and environmental security; security and continuity of supply; implementing, documenting, and maintaining action plans);
3) collecting information on cybersecurity threats and incident vulnerabilities;
4) handling incidents and collaborating with the relevant CSIRT in this regard; designating a contact person for the National Cybersecurity System (Ministry of Digital Affairs, 2025).

According to data for 2023, the number of entities in Poland with the status of essential service operators was approximately 400 (Ocena skutków, 2021). Essential service operators include entities such as: Wody Polskie, PGE Polska Grupa Energetyczna, Tauron Polska Energia, PKP Polskie Linie Kolejowe, Warszawskie Lotnisko Chopina, Orange Polska, Narodowy Fundusz Zdrowia.

The register of essential service operators is not public, publicly available, and is not published in the Public Information Bulletin. The data contained therein is made available only to entities specified in Article 7, paragraphs 7 and 8 of the Act of July 5, 2018, on the National Cybersecurity System.

Data from the register is made available by the minister responsible for computerization to computer security incident response teams: CSIRT MON, CSIRT NASK, and CSIRT GOV, as well as to sectoral cybersecurity teams within the sector or subsector for which they were established, as well as to the essential service operator to the extent applicable to it.

Additionally, the list of entities to which the list may be made available includes: cybersecurity authorities, the Police, the Military Police, the Border Guard, the Central Anticorruption Bureau, the Internal Security Agency and the Foreign Intelligence Agency, the Military Counterintelligence Service and the Military Intelligence Service, courts, the prosecutor's office, the National Revenue Administration, the Director of the Government Security Centre, and the State Protection Service.

Data from the list should be made available in accordance with the criterion of necessity for the performance of statutory tasks, as required by the constitutional principle of proportionality (Czaplicki, 2019)

It should be noted that the supervisory authority for cybersecurity is the minister responsible for IT. They oversee the internal structures established by the essential service operator and entities providing cybersecurity services to ensure: 1) the requirement to meet organizational and technical requirements to ensure cybersecurity for the essential service operator; 2) the requirement to have premises for providing incident response services that are secured against physical and environmental threats; 3) the requirement to apply security measures to ensure the confidentiality, integrity, availability, and authenticity of processed information, taking into account personal security, operation, and system architecture (Nowikowska, 2021).

3.2 Status of Essential Service Operators in Poland in the Context of the NIS 2 Directive

The previously mentioned NIS 2 Directive (Directive 2022/2555 of the European Parliament and of the Council concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive 2018/1972, and repealing Directive 2016/1148), adopted on December 14, 2022, introduces numerous changes to cybersecurity protection standards in Member States.

It indicates new directions for shaping European cybersecurity policy. First and foremost, the NIS 2 Directive eliminates the distinction between operators of essential services and digital service providers, which, as indicated above, remains in force in Polish law.

The preamble states that the NIS 2 Directive aims to address the shortcomings arising from the distinction between operators of essential services and digital service providers, which has proven outdated because it does not reflect the importance of the sectors or services concerned for social and economic activities in the internal market (Kurzępa-Piękoś, 2024).

In order to eliminate significant divergences between Member States in this respect and to provide legal certainty to all regulated entities with regard to cybersecurity risk management measures and incident notification obligations, it was necessary, in accordance with the provisions of the NIS 2 Directive, to establish a uniform criterion for determining which entities fall within the scope of this Directive.

According to the Union legislator, that criterion should provide for the introduction of a size rule, stipulating that the scope of this Directive covers all entities that qualify as medium-sized enterprises pursuant to Article 2 of the Annex to Commission Recommendation 2003/361/EC or that exceed the thresholds for medium-sized enterprises set out in paragraph 1 of that Article and that operate in the sectors covered by that Directive or provide the types of services or activities covered by it.

Member States should also ensure that certain small and micro-enterprises that meet specific criteria indicating their key role for society, the economy or specific sectors or types of services are included in the scope of this Directive (Directive 2022/2555).

The NIS 2 Directive therefore introduces the so-called size-cap principle, which essentially means that the directive covers all medium-sized and large enterprises operating in the sectors covered by the directive. This, in turn, means that security authorities will not designate, by administrative decision, entities that are subject to the rigors of the directive, and consequently, the Act on the National Cybersecurity System (Wrzosek, 2021).

The NIS 2 Directive introduced two types of entities: *essential entities* and *important entities*, thereby abandoning the previous distinction between operators of essential services and digital service providers. The essential entities, under the NIS 2 Directive, are entities from the following sectors: energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, and space. Pursuant to Article 3(2) of the NIS 2 Directive, entities of the type referred to in Annexes I or II of the Directive that do not qualify as essential entities are considered important entities.

The NIS 2 Directive expands the scope of the existing NIS Directive to include, among others, public administration, food, wastewater, industry, waste management, and space, and provides a broader coverage of certain sectors (including the extension of the scope of digital infrastructure) (Czekil, 2025). It also includes medium-sized and large enterprises in selected industries and allows a flexible approach to identifying smaller companies with a high-risk profile. The essential entities are, therefore, companies operating in areas such as energy, transportation, banking, digital infrastructure, healthcare, and public administration. Important sectors, in turn, include postal services, medical device manufacturing, DNS services (i.e., the Domain Name System), and waste management.

It should be noted that, in principle, small and micro-enterprises will not be subject to the provisions of the NIS 2 Directive, with the exception of entities that are trust service providers, DNS service providers, maintain TLD (i.e., top-level domain) registries, or perform other key functions within the digital sector (Czekil, 2025).

There is no doubt that the implementation of the NIS 2 Directive will require a larger number of organizations than previously recognized as entities within the national cybersecurity system.

This will also mean that numerous organizational units will have to bear significant financial burdens necessary to comply with the requirements set by the EU legislator. It should also be noted that entities regulated by the NIS 2 Directive will be required to implement advanced technical and organizational measures to manage cybersecurity risks and report incidents.

This includes, among other things, regular risk assessments, the implementation of security policies, ensuring supply chain continuity, and employee training. The new regulations emphasize a proactive approach to risk management and the continuous improvement of security measures. It will also be necessary to expand the powers of supervisory authorities to enforce regulations.

These powers include conducting inspections, audits, and requiring entities to document the implementation of adopted cybersecurity policies (BSJP, 2024). Significantly higher financial penalties are also envisaged for essential and important entities for non-compliance with selected provisions, which can reach up to €10 million or 2% of the total annual turnover for essential entities. Important entities may be fined up to €7 million or 1.4% of their total annual turnover (Article 34 of NIS 2 Directive).

As mentioned above, the deadline for implementing the NIS 2 Directive in European Union Member States is October 17, 2024. However, Poland and some other countries have not yet implemented the relevant changes to their national legal systems. It is expected that the NIS 2 Directive will likely be implemented in Polish law in the second quarter of 2025. During the period of work on implementing the directive, two key draft amendments to the Act on the National Cybersecurity System were developed.

The first draft of the Act, dated April 24, 2024, was met with significant public criticism and opposition from business circles and industry experts (Government Legislative Center, 2025). It was argued that the solutions proposed in this draft were more restrictive for entities covered by the national cybersecurity system than those resulting from the NIS 2 Directive (Government Legislative Center, 2025).

The concerns were primarily raised regarding the rules governing audits within the operations of entities covered by the national cybersecurity system. The stringent requirements for supply chain security also proved problematic, contributing to the final conclusion that the proposed project of changes to the national cybersecurity system may constitute too much of a burden, especially financial, for the entrepreneurs affected by the planned changes (Government Legislative Center, 2025).

Regarding the definition of essential entities in the aforementioned draft, it should be noted that for some of them, a size criterion was proposed, as adopted in the NIS 2 Directive (i.e., meeting the criteria for at least a medium-sized enterprise).

However, this status was also to be extended, regardless of company size, to DNS service providers, providers of managed cybersecurity services, qualified trust service providers within the meaning of Article 3(20) of Regulation 910/2014, critical entities, public entities, entities identified as essential entities pursuant to Article 7c(2)(1), and top-level domain name (TLD) registries.

However, such an exclusion remains consistent with the current provisions of the NIS 2 Directive, although it obviously significantly expands the scope of entities considered key in the national cybersecurity system.

Due to numerous critical comments regarding the first draft amendment to the Act on the National Cybersecurity System, the second draft was proposed on October 3, 2024, adapting Polish regulations to the requirements of the NIS 2 Directive. It harmonizes the list of sectors eligible for essential and important categories, in line with EU regulations, and limits supply chain security requirements solely to direct suppliers.

Furthermore, the attention was drawn to key statutory deadlines related to the implementation of the new obligations. Once the Act enters into force, essential and important entities will have three months to submit an application for entry into the appropriate list of entities, counting from that date or from the moment they meet the criteria for recognition as such.

It should be noted that under the current legal framework, which is still based on the implementation of the NIS Directive, such entry is made upon the request of the authority responsible for cybersecurity, submitted immediately after the issuance of a decision recognizing an entity as an essential service operator or a decision declaring the expiry of a decision recognizing an entity as an essential service operator.

If the latest draft law is passed, this obligation will be imposed on essential entities. According to the draft's assumptions of October 3, 2024, the deadline for implementing an information security management system is six months from the law's entry into force or from the moment these criteria are met.

A significant change compared to the first draft is the extension of the deadline for conducting the first audit for essential entities from 12 to 24 months, and the validity period of this audit has been extended from two to three years. These modifications give businesses more time to adapt to the new requirements, which should facilitate the effective implementation of necessary security measures (BJSP, 2024).

As for the definition of essential entities under the newly proposed solutions, it remains consistent with the one proposed in the draft act of April 24, 2024, but it also includes providers of managed cybersecurity services that at least meet or exceed the requirements for a small or medium-sized enterprise specified in Article 2(1) of Annex I to Regulation 651/2014/EU.

The list of entities that can obtain key entity status, regardless of size, has also been expanded to include: entities that are not entrepreneurs but have been recognized as essential entities pursuant to Annex 1 to the Act, either by name or by specifying their type; entities operating nuclear power facilities; and entities providing domain name registration services.

Furthermore, in accordance with the planned changes, electronic communications companies that at least meet or exceed the requirements for a medium-sized enterprise specified in Article 2(1) of Annex I to Regulation 651/2014/EU are also to be granted key entity status.

The bill is currently awaiting further proceedings in the Sejm (lower house of parliament). It is planned to be submitted to parliament later this year.

It should be noted that April 17, 2025, marks the 27-month deadline for European Union member states to establish a directory of essential and important entities (as well as those providing domain registration services). However, the form this directory will take in the context of Polish solutions remains unclear. Until this is established, the scope of the NIS Directive 2 cannot be definitively determined (Testarmy Group, 2025).

4. Conclusions

Essential service operators (ESOs) are entities, both public and private, that contribute to Poland's national cybersecurity system. They were first recognized in Polish law under the Act of 5 July 2018 on the National Cybersecurity System. The arguments presented in this publication support the thesis presented in the introduction: that they currently play a crucial role in ensuring the continuity and security of essential services that are crucial to the economy, public health, and social stability, while the legal framework for their operation remains broadly consistent with European Union standards.

ESOs are institutions providing services in areas such as energy, transport, water, ICT infrastructure, health, the banking sector, and public sectors that are essential to the functioning of the state and society. Their mission is to ensure the continuity of system operations and minimize the risk of disruptions that could have serious consequences. Among the most serious threats to the functioning of institutions with ESO status, cyberattacks are particularly noteworthy, which have intensified since the outbreak of the war in Ukraine.

Cyberattacks can result in data loss, management system failures, and, in extreme cases, even the paralysis of entire sectors. The responsibilities of essential service operators primarily concern infrastructure protection, risk assessment and crisis management in the event of incidents, and reporting serious incidents related to the operation of their systems.

The soon-to-be-released amendment to the Act of 5 July 2018 on the National Cybersecurity System will not only change the nomenclature of entities comprising the national cybersecurity system but will also lead to an increase in the number of entities deemed essential, and many businesses will face the need to implement new systems and solutions necessary for a cybersecurity policy aligned with the standards of the NIS 2 Directive.

The managers of essential and important entities will bear a significant burden of responsibility for the efficient functioning of the cybersecurity system in Poland. The planned changes, aligned with the requirements of the NIS 2 Directive, which are expected to enter into force in 2025, will therefore pose an organizational and financial challenge not only for state authorities but also for a large group of businesses.

It is anticipated that this situation will also lead to the emergence of a group of businesses specializing in providing services related to the implementation of new cybersecurity policy standards for institutions included in the list of essential and important entities. The effects of actual changes in the national cybersecurity system resulting from the implementation of the NIS 2 Directive, undoubtedly an interesting area of research, will only be assessed in the future, once the amendment to the Act on the National Cybersecurity System comes into force and is applied in the development of a new cybersecurity policy in Poland.

References:

Czaplicki, K. , Gryszczyńska, A. Szpor, G. 2019. Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, System Informacji Prawnej, LEX.

Czekil, P. 2025. Nowa Dyrektywa NIS 2 w 2025- kluczowe obowiązki dla przedsiębiorców, Available at: Nowa Dyrektywa NIS2 w 2025 – kluczowe obowiązki dla przedsiębiorców | inEwi Blog.

Czyżak, M. 2023. Odpowiedzialność karnoadministracyjna kierownika operatora usługi kluczowej za niezachowanie należytej staranności. Internetowy Kwartalnik Antymonopolowy i Regulacyjny. 4(12), 84-85. System Informacji Prawnej, LEX.

Górka, M. 2018. Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa. In: Dębowski, T. Cyberbezpieczeństwo wyzwaniem XXI wieku. Łódź-Wrocław, 31.

Kosior, E. 2020. Krajowy System Cyberbezpieczeństwa- zagadnienia wybrane. In: Pomykała, M., Merkwa, M. Nowe technologie- współczesne wyzwania w obszarze prawa i bezpieczeństwa. Rzeszów, 18.

Kurzępa-Piękoś, E. 2021. Dyrektywa NIS oraz NIS 2 w kontekście cyberbezpieczeństwa w Polsce. In: Jurgilewicz, O., Kozicki, B., Woźny, A. Współczesne konteksty bezpieczeństwa. Rzeszów, 21-22.

Mąkosa, G. 2021. Bezpieczeństwo cyberprzestrzeni Rzeczypospolitej Polskiej. Studia Bezpieczeństwa Narodowego, 22. Warszawa.

Nowikowska, M. 2021. Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa. Cybersecurity and Law, 1(5), 77-103.

Oleksiewicz, I. 2020. Cyberbezpieczeństwo i sztuczna inteligencja w sektorze energetycznym UE. Rocznik Bezpieczeństwa Międzynarodowego, 14 (1), 229.

Oleksiewicz, I. 2020. Reforma polityki cyberbezpieczeństwa Unii Europejskiej. In: Teka of Political Science and International Relations, 15/2, 12.

Wąsowski, K. 2021. Tasks of the Minister of National Defence in the Field of Cybersecurity. In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. Cybersecurity in Poland. Legal aspects. Available at: Tasks of the Minister of National Defence in the Field of Cybersecurity | SpringerLink.

Woszek, S. 2022. Cyberbezpieczenstwo państwa w XXI wieku na przykładzie Rzeczypospolitej Polskiej. Przegląd Bezpieczeństwa Wewnętrznego, 27 (14), 202-203.

Wrzosek, M. 2021. Dyrektywa w sprawie odporności podmiotów krytycznych i Dyrektywa NIS 2- nowe wyzwania dla operatorów w zakresie cyberbezpieczeństwa. Nowa Energia, 5-6(81), 66.

Vacca, W.A. 2011. Military Culture and Cyber Security. Survival Global Politics and Strategy, 53/6, 159-176.

Legal acts:

Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, OJ 2016, L 194/1.

Directive (EU) 2022/2555 of the European Parliament and of the Council concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ 27 December 2022, L 333/80.

Act of 5 July 2018 on the National Cybersecurity System, OJ 2024, item 1077, as amended. • Justification for the draft Act of July 5, 2018, on the national cybersecurity system, the LEX Information System.

Resolution No. 125 of the Council of Ministers of October 22, 2019, on the Cybersecurity Strategy of the Republic of Poland for 2019-2024, Journal of Laws of 2019, item 1037.

Internet sources:

BSJP, 2024. Dyrektywa NIS 2 w Polsce- założenia i stan prac nad jej implementacją Dyrektywa NIS2 w Polsce: założenia i stan prac nad jej implementacją. Available at: Dyrektywa NIS2 w Polsce: założenia i stan prac nad jej implementacją

Government Legislative Center, 2025. Projekt ustawy z dnia 24 kwietnia 2024 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Available at: https://legislacja.gov.pl/projekt/12384504/katalog/13055207

Ministry of Digital Affairs, 2025, Available at: Operatorzy Usług Kluczowych - Ministerstwo Cyfryzacji - Portal Gov.pl

Ministry of Infrastructure, 2025, Available at: Informacje bieżące - Ministerstwo Infrastruktury - Portal Gov.pl

Ocena skutków regulacji Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. 2021. Available at: f1c175f525e236f616ee5843b457c4a6.pdf

Testarmy Group, 2025. NIS 2. Podmioty kluczowe i ważne. Czyli kto? Available at: NIS 2. Podmioty kluczowe i ważne. Czyli kto? - Testarmy Group.