REVIEW OF EUROPEAN AND COMPARATIVE LAW
VOLUME XLVI
YEAR 2021, ISSUE 3, pp. 219–235
DOI: https://doi.org/10.31743/recl.12645

THE EVOLUTION OF CYBERSECURITY REGULATION IN THE EUROPEAN UNION LAW AND ITS IMPLEMENTATION IN POLAND

*Grażyna Szpor**

ABSTRACT

The 2013 European Union Cybersecurity Strategy, the 2016 Directive, and the 2019 Regulation mark the next steps in strengthening the protection of cybersecurity by European Union bodies, linked to changes in member states' laws. The rapid increase in threats, referred to as the "cyberpandemic", requires prompt adaptation of legal instruments to new needs, but at the same time complicates ensuring consistency of multi-level regulation. The analysis of changes in the legal status in Poland shows that this concerns terminology, subject matter scope and the structure of cyber security systems. In order to reduce difficulties, it is worth considering introducing immediate amendments to those provisions in force which were negatively assessed during works on drafting new acts. Such a conclusion is prompted by the evolution of the definition of cybersecurity, which, according to the 2019 Regulation as well as the draft amendments to the Polish Act on National Cyber Security System and the draft of the new Directive, is to be understood as activities necessary to protect networks and information systems, users of such systems and other persons against cyber threats such as any potential circumstance, event or action that may cause damage, disruption or otherwise adversely affect networks and information systems. Another example is the maintenance of the distinction between key service operators and digital service providers in the 2019 EU Regulation and the 2021 draft amendment to the Polish law,

* Prof. Dr. habil. Grażyna Szpor, Professor, Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw; correspondence address: Woycickiego 1/3/17, 01-938 Warszawa, Poland; e-mail: g.szpor@uksw.edu.pl; https://orcid.org/ 0000-0002-3264-9360.

although the 2020 NIS 2 directive draft recognizes that it has become irrelevant and replaces it with a distinction between essential and relevant entities. Also, other changes currently proposed are justified by the blurring of the boundaries between virtual and real space.

Keywords: cybersecurity, cyberspace, legislation, NIS Directive, ENISA

1. INTRODUCTION

Cybersecurity is currently the subject of intense legislative regulation in international, EU and domestic law. This paper seeks to verify the claim that the conceptual network, scope and structure of this regulation have a number of shortcomings that ought to be mitigated in order not to compromise its effectiveness. The achievement of this goal requires the application of legal research methods, primarily the dogmatic and comparative methods, as well as big data analysis.

2. LEGAL INSTRUMENTS CONCERNING CYBERSECURITY

Over the past quarter of a century, efforts have been made to provide a legal framework for the security of electronic network communication, and by now the regulatory landscape contains instruments of multiple levels, but they are assessed critically[1].

Since the second half of the 20th century, the United Nations General Assembly has adopted a number of resolutions and other soft law acts, but the ambition to regulate the issue in question by way of a global convention have never materialized. Relating general acts to cyberspace encounters difficulties, including those related to the attribution of cyber-

[1] Cf. Ansgar Baumgarten and Christian Calliess, "Cybersecurity in the EU the Example of the Financial Sector: A Legal Perspective," *German Law Journal* 21, no. 6 (2020): 1149–1179; Kamil Czaplicki, Agnieszka Gryszczyńska, and Grażyna Szpor, eds., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warsaw: Wolters Kluwer Polska, 2019); Jeff Kosseff, "Hamiltonian Cyversecurity," *Wake Forest Law Review* 54, no. 1 (2019): 155–206; H. P. Singh and Tareq S. Alshammari, "An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia," *Beijing Law Review* 11, no. 3 (2020): 637–650.

space to states. Dynamic interpretation and case law assist in overcoming these problems[2]. In international law, the principal legally binding act, but with regional reach, is the Council of Europe Convention on Cybercrime, made on 23.11.2011 in Budapest, to which a draft Second Additional Protocol has been in preparation since 2017[3].

In European Union law, the two principal instruments are 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 (NIS Directive)[4], and Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[5]. Work on NIS 2 was still ongoing in 2021[6].

---

[2] Przemysław Roguski, "Przesłanki przypisania cyberoperacji państwu," in *Internet. Cyberpandemia*, ed. Agnieszka Gryszczyńska and Grażyna Szpor (Warsaw: C.H. Beck, 2020), 91–101; Joanna Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy* (Warsaw: Wolters Kluwer Polska, 2020).

[3] Andrzej Adamski, "Europejskie standardy prawno-karnej ochrony sieci i informacji oraz ich implementacja do prawa polskiego," in *Internet. Strategie bezpieczeństwa*, ed. Agnieszka Gryszczyńska and Grażyna Szpor (Warsaw: C.H. Beck, 2017), 23–46; Information on a proposition of a draft Second Additional Protocol to the Convention on Cybercrime (ETS 185); https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

[4] 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 (NIS Directive) (OJ L 194 of 19.07.2016, p. 1). It was created in implementation of the provisions adopted on 7.02.2013. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions /* Join/2013/01 Final */.

[5] OJ L 2019/L151/15.

[6] Proposal for a Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final); Cf. The EU's Cybersecurity Strategy for the Digital Decade. Joint Communication to the European Parliament and the Council Brussels of 16.12.2020 (COM/2021/118 final).

In Polish domestic law, the Act on the National Cybersecurity System[7] of 5 July 2018 implements the NIS Directive, but its scope actually exceeds the requirements of this directive. Works on the amendment of this act began in 2020[8].

Efforts to improve the regulation of cybersecurity undertaken in 2021 in international, European and domestic law, encompassed the amendment of existing laws and the drafting of new ones[9]. This intensification was a result of the "cyber pandemic". This term refers to the similarities between cyber-attacks and any pandemic (not only COVID-19), including the results of their global and rapid spread that are devastating to people and the economy. The massive and sudden shift from the virus-ridden reality to cyberspace has heightened the awareness of opportunities associated with this digital transformation, especially as regards healthcare. It has also revealed the insufficient preparation for safe use of cyberspace, increased the activity of cybercriminals, and made higher cybersecurity a key task for public authorities, businesses and citizens, confirming the validity of theoretical observations on valorization of deficits[10]. The increasingly intrusive cyber-attacks prompt 'active defence' and 'pre-emptive defence' by public authorities, but these are also becoming attractive to global corporations active on the Internet. Achieving acceptable regulatory effectiveness is important to avoid 'companies starting a war'[11].

---

[7] Act of 5 July 2018 on the National Cybersecurity System (consolidated text: Journal of Laws of 2020, item 1369).

[8] Draft act amending the Act on the National Cybersecurity System and of the Act on Public Procurement of 7 September 2020, as well as a separate draft Act on Electronic Communication of 29 July 2020; next draft act amending the Act on the National Cybersecurity System and of the Act on Telecommunications of 20 January 2021; https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html.

[9] The EU is working on two legislative proposals to address current and future online and offline risks: an updated directive to better protect network and information systems a new directive on the resilience of critical entities, https://www.consilium.europa.eu/en/policies/cybersecurity/.

[10] Agnieszka Gryszczyńska and Grażyna Szpor, eds., *Internet. Cyberpandemia* (Warsaw: C.H. Beck, 2020).

[11] Brian Corcoran, "A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace," *Harvard National Security Journal* 11, no. 1 (2020): 2.

3. THE TERM 'CYBERSECURITY' AND ITS DEFINITIONS

Brian Corcoran, while admitting that 'cyber' is a notoriously unclear term, adopts that "it simply means 'pertaining to the Internet'". The terms 'cyberattack' and 'cyberwar' are even more vague[12].

In 2021, the 'cyber-' prefix could be found in a few hundred Wikipedia entries, and it generated ca. 1.76 billion search results in Google[13], and so it is important for the clarity of law to agree on the definitions of those terms that contain said prefix.

The term 'cybersecurity' was included in the title of the 2013 EU strategy. However, it was missing from the 2016 NIS Directive which embodied the provisions of this strategy, as a definition consensus could not be reached. Two years later, in 2018, it was once again used in the title of the Polish act implementing this directive, in which it was defined. Nevertheless, in 2019 cybersecurity was introduced into the abbreviated title of the Regulation of the European Parliament and Council (EU) 2019/881, in which it was defined differently than in the Polish act. In December 2020, it once again appeared in the subsequent EU's Cybersecurity Strategy for the Digital Decade[14].

In the Polish Act of 5 July 2018 on National Cybersecurity System (Art. 2(4)), cybersecurity is defined as the resilience of information systems against any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services

[12] Corcoran, "A Comparative Study of Domestic Laws," 5.

[13] Search result of 28 March 2021.

[14] Joint Communication to the European Parliament and the Council, Brussels, 16.12.2020 (COM/2021/118 final), https://www.consilium.europa.eu/en/policies/cybersecurity/: "In December 2020, the European Commission and the European External Action Service (EEAS) presented a new EU cybersecurity strategy. The aim of this strategy is to strengthen Europe's resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The new strategy contains concrete proposals for deploying regulatory, investment and policy instruments. On 22 March 2021, the Council adopted conclusions on the cybersecurity strategy, underlining that cybersecurity is essential for building a resilient, green and digital Europe. EU ministers set as a key objective achieving strategic autonomy while preserving an open economy. This includes reinforcing the ability to make autonomous choices in the area of cybersecurity, with the aim to strengthen the EU's digital leadership and strategic capacities".

offered by those information systems. This is similar to the definition of networks and systems security in the implemented NIS Directive, but not identical[15].

In a later EU Regulation 2019/881, which is directly applicable in the national legal order, 'cybersecurity' is defined as activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats. A 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

There are significant differences between these definitions. Pursuant to the Act on the National Cybersecurity System, cybersecurity is a goal to be achieved (resilience), and pursuant to Resolution 2019/881, cybersecurity comprises activities. Resilience applies only to information systems and activities apply to networks and information systems, but also separately to their users and others. Resilience is concerned with breaches and activities are concerned with protection against cyber threats, covering potential circumstances, an event or an action. Pursuant to the Polish act, the confidentiality, integrity, availability and authenticity of the processed data or related services offered by information systems may be breached, while the regulation more generally indicates the risk of damage, disruptions or other adverse effects on networks, systems and persons, also those who are not users of networks and systems[16].

The postulate of ensuring coherence of multi-level regulation by way of disambiguation of the term 'cybersecurity' was not accounted for in the original draft amendment of the Act on the National Cybersecurity System of 7 September 2020. It was, however, included in the draft amendment of 20 January 2021, where Art. 2(4) of the Act on the National Cybersecurity System was given the following wording: "(4) cybersecurity - measures necessary to protect information systems, users of such

[15] Grażyna Szpor, "Komentarz do art. 2," in *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. Kamil Czaplicki, Agnieszka Gryszczyńska, and Grażyna Szpor (Warsaw: Wolters Kluwer Polska, 2019).

[16] Grażyna Szpor, "Nowelizacja siatki pojęciowej cyberbezpieczeństwa," *Monitor Prawniczy*, no. 22 (2020): 1189.

systems and other persons from cyber threats". Also, the following point 4a has been added: "(4a) information systems security - the resilience of information systems to actions that compromise the confidentiality, integrity, availability and authenticity of the data processed or the related services offered by those systems". It seems as though the definition of cybersecurity from Regulation (EU) 2019/881 might be consolidated in this respect in the NIS 2 Directive[17], which may facilitate distinguishing cybersecurity in statistics as a separate sector of the economy[18].

Some words, however, have been translated incorrectly in the Official Journal of the European Union. For example, cybersecurity has been translated as *bezpieczeństwo cybernetyczne* instead of *cyberbezpieczeństwo*, and information systems have been translated as *systemy informatyczne* instead of *systemy informacyjne*. A corrigendum procedure must be urgently implemented to fix these errors, not only because of the Act on the National Cybersecurity System[19]. The weight of translation problems is also confirmed by a proposal of a new approach to them set forth in the draft Second Additional Protocol to the Budapest Convention[20].

'Cybersecurity' is a commonly used term in scholarly publications, education, names or organizational units and in colloquial language: in

[17] Art. 4(3) of the proposal for a Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final); https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020PC0823&qid=16178372001 defines 'cybersecurity' as cybersecurity within the meaning of Art. 2(1) of Regulation (EU) 2019/881, while pursuant to Art. 4(7), A 'cyber threat' is a cyber threat within the meaning of Art. 2(8) of Regulation (EU) 2019/881.

[18] Consolidated text: Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02006R1893–20190726&qid=1620666649813.

[19] Changing the statutory Polish definitions of *system informatyczny* and *system teleinformatyczny* could be an alternative to the corrigendum regarding systems. Cf. Szpor, "Nowelizacja siatki pojęciowej cyberbezpieczeństwa," 1191.

[20] Information on a proposition of a draft Second Additional Protocol to the Convention on Cybercrime (ETS 185); https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

2021, it rendered about 137 million Google search results[21]. Although its introduction to the legal language raised some doubts, in 2021 EUR-LEX search engine turned up ca. 1300 documents that contain this word. This confirms the thesis that we need a short collective term, and that alternatives are unattractive. We also need disambiguation and coherence of other terms with the cyber- component, such as cyber threat, cyber-attack, cyberoperations, cybercrime, cyberspace, etc. Initial works on a cybersecurity lexicon have also revealed that these terms are used inconsistently in legal instruments, official documents and normalization, and it is a problem that needs addressing.

4. AIM, SCOPE AND REMEDIES IN CYBERSECURITY

Art. 1 of the NIS Directive specifies its aim to be the achievement of a high common level of security of network and information systems (par. 1), as well as five means to this end (par. 2, a-e).

In the Polish Act on the National Cybersecurity System of 5 July 2018, which implements the NIS Directive into the Polish legal order, the aim may only be deduced from the definition of cybersecurity as provided in Art. 2. Art. 1(1) of the Polish act succinctly lays down its subject matter as concerning the "organisation of a national cybersecurity system and the tasks and duties of entities forming part of this system" (p. 1), as well control and oversight (p. 2) and strategy (p. 3), which does not reflect the act's structure. The draft amendment of 2021 broadens the subject matter and scope to include the organisation of the national cybersecurity certification system and the rules and procedures for the certification of an ICT product, ICT service or ICT process for cybersecurity as defined in Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019[22].

[21] Cybersecurity – ca.137,000,000 results; *cyberbezpieczeństwo* – ca.1,500,000 results; Search performed on 28.03.2021.

[22] "The following amendments are introduced to the Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws of 2020, item 1369): 1) In Art. 1: a) point 1a in the following wording is added after point 1 of par. 1: "(1a) the organisation of the national cybersecurity certification system and the rules and procedures for the cer-

The subjective scope of the NIS Directive is narrower than its drafts had envisaged[23]. However, since the Directive was based on the principle of minimum harmonisation, under Article 3 Member States may, without prejudice to Article 16(10) and to their obligations under EU law, adopt or maintain provisions aimed at achieving a higher level of security of networks and information systems. In Poland, this option was used to broaden the subjective scope. In addition to 6 sectors of the economy considered crucial for the socio-economic security of the state, i.e.: Energy, Transport, Health, Banking and Financial Markets Infrastructure, Water Supply and Digital Infrastructure, also most entities of the public finance sector were included in the scope of the original version of the Act on the National Cybersecurity System. The 2021 amendment draft has introduced some exceptions to the earlier exclusion of telecommunications and trust service providers from the scope of the act[24].

The NIS 2 proposal, however, ushers in further-reaching changes. The impact assessment of the existing directive found it to be too limited

---

tification of an ICT product, ICT service or ICT process in the field of cybersecurity as defined in Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act) (OJ L 151 of 07.06.2019, p. 15), hereinafter referred to as "Regulation 2019/881".

[23] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM/2013/048 final 2013/0027.

[24] "Par. 2(1) is given the following wording: "1) telecommunications entrepreneurs referred to in the Act of 16 July 2004 - Telecommunications Law (Journal of Laws of 2019, item 2460 and of 2020, item 374, 695 and 875), with regard to security requirements and incident reporting with the exception of Articles 66a-66c, Articles 67a-67b and Articles 73–74", in par. 2, point 2 is given the following wording: "2) trust service providers who are subject to the requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257 of 28.08.2014, p. 73) with the exception of Articles 67a-67b and Articles 73–74"; Draft of 20 January 2021 of the Act on amending the Act on the National Cybersecurity System and the Act on Telecommunications, https://www.gov.pl/web/krmc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-telekomunikacyjne.

mainly due to increased digitisation in recent years and a higher degree of interconnectedness[25]. The new directive is to apply to certain public and private "essential entities" operating in sectors listed in Annex I (energy; transport; banking; financial markets infrastructure; health care; drinking water; waste water; digital infrastructure; public administration and space), as well as to certain "important entities" operating in the sectors listed in Annex II (postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; digital providers). The proposal excludes micro and small entities within the meaning of the Commission Recommendation of 6 May 2003 2003/361/EC from the Directive scope, with the exception of providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration, and certain other entities, such as the sole provider of a service in a Member State. Recital 7 of the preamble states that the sectors covered by the directive should be extended to provide a comprehensive coverage of the sectors and services of vital importance. Moreover, the rules should not be different according to whether the entities are operators of essential services or digital service providers, as this differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.

In a bid to increase the consistency of imposing directive obligations in individual Member States, it was decided that uniform criterion should be established that determines the entities falling within the scope of application of this Directive based on their size. Specifically, all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC 15, that operate within the sectors or provide the type of services covered by this directive, fall within its scope, with no additional actions required on the part of Member States. On the other hand, it has been left up to Member States to establish lists of micro and small entities with a key role

[25] Impact assessment 7, which was submitted to the Regulatory Scrutiny Board (RSB) on 23 October 2020 and received a positive opinion with comments by the RSB on 20 November 2020; Cf. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

for the economies or societies of Member States or for specific sectors or types of services, which should be covered by the directive, and to submit such lists to the Commission[26].

The analysis of the evolution of cybersecurity regulation shows that it is expanding rapidly both in terms of its objective and subjective scope, and that efforts are under way to achieve uniform cybersecurity obligations for companies across the European Union. However, the quickly changing cyber landscape makes it difficult to achieve consistency between European and domestic laws and defers the achievement of uniformity between Member States' national regulations. In Poland, the amendment of the 2018 Act to align with the 2019 EU Regulation will likely be ready shortly before the repeal of the NIS Directive that it implemented into national law, followed by the adoption of the new NIS 2 Directive, the transposition of which will force further changes to domestic law[27]. Problems in trans-border relations may also be triggered by the fact that the NIS 2 Directive will be transposed at different times in the Member States, as the proposal for this directive provides for a time limit of 18 months following its adoption for this procedure to be completed.

5. CYBERSECURITY SYSTEM STRUCTURE

The NIS Directive has designated the following entities tasked with ensuring EU-wide cooperation in the area of network and information systems security: The Cooperation Group (composed of representatives of Member States, the Commission and the European Union Agency for Cybersecurity (ENISA)) and a computer security incident response team (CSIRT) network, for which ENISA is to provide the secretariat

[26] Cf. recitals 8 and 9 of the preamble of the Proposal for a Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final).

[27] Pursuant to the proposal, the Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148, enters into force on the twentieth day following that of its publication in the Official Journal of the European Union (Art. 42), and Member States have 18 months for its transposition, upon the lapse of which the NIS Directive ceases to have effect.

(Chapter 3). The 2019 ENISA regulation brought about a strengthening of cooperation, and NIS 2 introduces new solutions in this regard, meant in particular to strengthen ties with the institutional environment. The entities of cooperation according to the draft NIS 2 are the Cooperation Group (CG) with an expanded composition[28], the CSIRTs network[29] and a new entity: a European Cyber Crises Liaison Organisation Network (EU - CyCLONe), composed of representatives of Member States crisis management authorities, the Commission and ENISA[30].

Simultaneously with the proposal on NIS 2, on 16.12.2020 the Commission submitted a proposal for a directive on the resilience of critical entities[31]. It is emphasized that this proposal is consistent and establishes close synergies with the proposed NIS 2 Directive, which will replace the NIS Directive in order to address the increased interconnectedness between the physical and digital world through a legislative framework

[28] Pursuant to Art. 12 of the Proposal for a Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive (ENISA) 2016/1148 (COM/2020/823 final), the Cooperation Group is to be composed of representatives of Member States, the Commission and ENISA. The European External Action Service is to participate in the activities of the Cooperation Group as an observer. Pursuant to proposal for a regulation on the digital operational resilience for the financial sector, also the European Supervisory Authorities may participate in the activities of the Cooperation Group. The Cooperation Group is to meet at least once a year with the Critical Entities Resilience Group established under directive on the resilience of critical entities.

[29] Pursuant to Art. 13 of the Proposal for a Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final), the CSIRTs network will be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission is to participate in CSIRTs network work as an observer. ENISA is to provide the secretariat.

[30] Pursuant to Art. 14 of the Proposal for a Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final); EU-CyCLONe will have the following tasks: (a)increasing the level of preparedness of the management of large scale incidents and crises; (b)developing a shared situational awareness of relevant cybersecurity events; (c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis; EU-CyCLONe will cooperate with the CSIRTs network. ENISA, among others, is to provide the secretariat.

[31] Cf. Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (COM/2020/829 final).

with robust resilience measures, both for cyber and physical aspects as set out in the Security Union Strategy"[32].

In 2016, the NIS Directive indicated the following national entities to be designated: one or more national competent authorities on the sectors and services covered by the scope of the directive, a national single point of contact acting as a liaison to ensure cross-border cooperation[33], and one or more CSIRTs. It also imposed specific obligations concerning network and systems security on two categories of entities: 'operators of essential services' and 'digital service providers'.

The 2018 Act on the National Cybersecurity System contains a 20-point enumeration of the types of entities covered by this system (Art. 4), but they are not structured in any way. Commentaries to the Act, departing from the statutory definition of cybersecurity as the goal to be achieved, distinguish three categories of these entities: administration bodies responsible for the cybersecurity of other entities within the system (including competent authorities and CSIRTs); entities obliged to protect their own cybersecurity in the public interest (including operators of essential services, digital services providers and public entities), as well as entities specializing in providing services in support of cybersecurity[34].

After two years since its entry into force, the Act has been assessed critically in Poland. Some critics have pointed out that, with the exception of the financial sector, the statutory option to designate sector-wide cybersecurity teams supporting operators of essential services has not been taken, even though some such operators have difficulties meeting the technical

[32] Cf. Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (COM/2020/829 final).

[33] 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 (NIS Directive) (OJ L 194 of 19.07.2016, p. 1).

[34] Grażyna Szpor, "Komentarz do art. 4," in *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. Kamil Czaplicki, Agnieszka Gryszczyńska, and Grażyna Szpor (Warsaw: Wolters Kluwer Polska, 2019); Cf. Agnieszka Besiekierska, ed., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warsaw: C.H. Beck, 2019); Waldemar Kitler, Joanna Taczkowska-Olszewska, and Filip Radoniewicz, eds., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warsaw: C.H. Beck, 2019); Cezary Banasiński and Marcin Rojszczak, eds., *Cyberbezpieczeństwo* (Warsaw: Wolters Kluwer, 2020).

requirements of internal cybersecurity structures. In the public sector, uncompetitive salaries made it difficult to recruit specialists, and provincial authorities failed to ensure adequate response to incidents in municipalities and coordination of information security activities. Only one ISAC (Information Sharing and Analysis Center) was established (Rail ISAC). The Government Commissioner for Cybersecurity lacked effective means to influence the actors of the national cybersecurity system[35].

The draft amendment of the Act on the National Cybersecurity System, adjusting its provisions to the requirements of the ENISA regulation, provided for the mandatory establishment of sectoral CSIRTs, the inclusion in the system of 16 local government administration bodies - provincial governors, mandatory support for operators of essential services by operational security centres (OSCs, which decide on the implementation of security measures based on risk assessment), and the provision of expert support by several dozen registered ISACs (centres for exchange and analysis of information on vulnerabilities, cyber threats and incidents). Moreover, types of entities covered by the national cybersecurity system, especially operators of essential services, digital services providers and telecommunications entrepreneurs (who are large companies) will have to withdraw given equipment or software from use within 7 years of a relevant risk assessment decision issued by the minister responsible for informatization (high-risk providers)[36]. Failure to comply with the obligation to withdraw ICT products, services and processes of a high-risk provider, as well as failure to comply with the obligation to perform a certain action specified in the security order is to be subject to a fine of up to 3% of the total annual worldwide turnover from the preceding financial year. Other MS were also still working on the transposition of Regulation

[35] Draft act amending the Act on the National Cybersecurity System and of the Act on Telecommunications of 20 January 2021; https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html, p. 90–91.

[36] Telecommunications entrepreneurs who have or use the types of ICT products, types of ICT services, specific ICT processes indicated in the decision and specified in the list of categories of critical functions for network and service security in Annex No. 3 to the Act will have to withdraw them within 5 years from the announcement of the decision.

2019/881 in 2021. The draft laws contained different detailed solutions. The level of their progress varied[37].

The proposed amendment to the Polish Act introduces new instruments of mitigating dysfunctions identified in the impact assessment of the existing regulation. However, its amended version may be in force soon, while draft NIS 2 Directive eliminates the categories of operators of essential services and digital service providers, instead adopting the distinction between 'essential entities' and 'important entities'[38] based on how critical the sector or type of service is, and accounting for how heavily other sectors and services rely on them[39]. The NIS 2 Directive also stipulates that public authorities will be able to order the withdrawal of products and services of IT operators qualified as high-risk providers, and it too provides for high penalties for the failure to oblige. The dynamics of change increases the importance of confronting national legislative work with the prospect of changes to European law. Strengthening the role of specialised services in the sphere of cybersecurity, understood as a type of activity, also underlies the postulate to separate cybersecurity in statistical classifications of economic activity[40].

[37] Draft Act of 20 January 2021 amending the Act on the National Cybersecurity System and the Act on Telecommunications, Regulatory Impact Assessment (pp. 89–91), https://www.gov.pl/web/krmc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-telekomunikacyjne.

[38] Pursuant to Art. 4(25) of the Proposal for a Directive of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final); an 'essential entity' means any entity of a type referred to as an essential entity in Annex I. Pursuant to Art. 4(26), an 'important entity' means any entity of a type referred to as an important entity in Annex II. The division criterion is clarified in recital 11 of the preamble.

[39] Cf. Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (COM/2020/829 final).

[40] Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains (OJ L of 2006, No. 393, p. 1 as amended); Cf. Szpor, "Nowelizacja siatki pojęciowej cyberbezpieczeństwa," 1190.

6. CONCLUSIONS

The 2016 NIS Directive ushered in a period of intensified work in the area of regulating cybersecurity, with a host of new laws and amendments of existing ones, both on the EU and domestic level. The changes, those already made and those proposed, enhance terminological integrity, as well as broaden and unify the subject and entity scope of cybersecurity systems across EU Member States. They also increase the obligations to reduce cyber threats and strengthen the instruments that public authorities have at their disposal to enforce these obligations.

Reconciling demands for rapid adaptation of regulations to new needs with the principles of stability, consistency and transparency of law as conditions for its effectiveness requires breaking the separation and improving the coordination of parallel legislative processes.

REFERENCES

Adamski, Andrzej. "Europejskie standardy prawno-karnej ochrony sieci i informacji oraz ich implementacja do prawa polskiego." In *Internet. Strategie bezpieczeństwa*, edited by Agnieszka Gryszczyńska and Grażyna Szpor, 23–46. Warsaw: C.H. Beck, 2017.

Banasiński, Cezary, and Marcin Rojszczak, eds. *Cyberbezpieczeństwo*. Warsaw: Wolters Kluwer, 2020.

Baumgarten, Ansgar, and Christian Calliess. "Cybersecurity in the EU the Example of the Financial Sector: A Legal Perspective." *German Law Journal* 21, no. 6 (2020): 1149–1179.

Besiekierska, Agnieszka, ed. *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warsaw: C.H. Beck, 2019.

Corcoran, Brian. "A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace." *Harvard National Security Journal* 11, no. 1 (2020): 1–ix.

Czaplicki, Kamil, Agnieszka Gryszczyńska, and Grażyna Szpor, eds. *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warsaw: Wolters Kluwer Polska, 2019.

Gryszczyńska, Agnieszka, and Grażyna Szpor, eds. *Internet. Cyberpandemia*. Warsaw: C.H. Beck, 2020.

Kitler, Waldemar, Joanna Taczkowska-Olszewska, and Filip Radoniewicz, eds. *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warsaw: C.H. Beck, 2019.

Kosseff, Jeff. "Hamiltonian Cybersecurity." *Wake Forest Law Review* 54, no. 1 (2019): 155–206.

Singh, H. P., and Tareq S. Alshammari. "An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia." *Wake Forest Law Review* 11, no. 3 (2020): 637–650.

Szpor, Grażyna. "Nowelizacja siatki pojęciowej cyberbezpieczeństwa." *Monitor Prawniczy* 22 (2020): 1189–1192.

Roguski, Przemysław. "Przesłanki przypisania cyberoperacji państwu." In *Internet. Cyberpandemia*, edited by Agnieszka Gryszczyńska and Grażyna Szpor, 91–101. Warsaw: C.H. Beck, 2020.

Worona, Joanna. *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*. Warsaw: Wolters Kluwer Polska, 2020.