„Polityka i Społeczeństwo" 2(22) / 2024
DOI: 10.15584/polispol.2024.2.16

ARTYKUŁY

Tomasz Skrzyński*

LEGAL AND ORGANIZATIONAL ASPECTS OF COUNTERING THREATS TO THE EU'S CRITICAL INFRASTRUCTURE AFTER THE 24TH OF FEBRUARY 2022

Abstract

Given the importance of Critical Infrastructure, safeguarding its security occupies a prominent place on the EU's political agenda. The current confrontation between the West and Russia has led to a significant tightening of regulations and increased expenditure, aimed at enhancing the resilience of Critical Infrastructure against threats. Despite legal and organizational efforts, over a medium-term perspective, the current economic situation is significantly hampering efforts to continue high level of funding for various aspects of CI protection in EU member states.Varying levels of determination on the part of national governments to enforce regulations and deliver action on CI protection are another factor that undermines the effectiveness of measures at EU level. These are due, amongst others, to individual governments' assessment of threat posed by Russian and Chinese policies as well as different scales of threat posed by Russia to individual member states' CI. Another challenge is constituted by different levels of the effectiveness of the machinery of government in individual EU member states.

Keywords: information security, Critical Infrastructure, European Union, consequences of Russian aggression against Ukraine in 2022

Introduction

Rapid advances in telecommunications, ICT, financial, transport and health care technologies as well as the scale of advancement in industrial process digitization and the presence of large corporations therein are producing various consequences. On one hand, they allow Critical Infrastructure (CI) to be better monitored and make it possible to respond very quickly to improper operation or disruptions in the operation of CI systems and facilities[1]. On the other hand, they increase

* Uniwersytet Komisji Edukacji Narodowej w Krakowie, e-mail: tomasz.skrzynski @uken.krakow.pl, ORCID: 0000-0003-2063-4396

the level of dependence on CI on the part of the economy, communities and individuals[2].

At the same time, the continuously growing, fast-paced integration between different CI subsystem entities intensify the consequences of attacks and breakdowns of facilities included in CI. Although an initial attack may target a single system, it is likely to quickly propagate to a vast geographical area and severely hamper the operation of other systems.

CI is of particularly great importance to the functioning of highly developed countries[3]. Countering information threats against CI is a very important component of efforts to strengthen the EU's resilience in the face of Russia's aggressive policy[4] as Russia's downright aggression against Ukraine has increased the likelihood of massive damage to civil systems and facilities that are key to the security of EU member states and their citizens[5]. Furthermore, action to maintain EU member states' defence capabilities is particularly important for strengthening CI resilience.

Countering threats against CI can be analysed, among other things, from a political, economic or a functional perspective, or in terms of state security. There are various CI protection models (e.g. integral, centralized, decentralized)[6]. Legal and organizational measures need to take into consideration quantitative and functional parameters of individual

[1] More extensively on CI and the key threats to its functioning: R. Wódkiewicz, *Podstawowe zagrożenia funkcjonowania obiektów Infrastruktury Krytycznej*, „Zeszyty Naukowe SGSP", 2022, no 83, pp. 141–161.

[2] J. Falecki, *Ochrona Infrastruktury Krytycznej*, [in:] *Encyklopedia Bezpieczeństwa*, eds O. Wasiuta, S. Wasiuta, v. 5, Kraków 2022, p. 543.

[3] D. Juristic, *Challenges of Critical Infrastructure protection in contemporary security environment*, [in:] *Security and crisis managementtheory and practice 9th International Scientific and Professional Conference 29.09.2023. and 30.09.2023*, p. 6. ResearchGate, https://www.researchgate.net (01.12.2023).

[4] Synthesis on the evolution of Russia's information security policy in the 21st century: Saalman, Fei Su, L.S. Dovgal, *Cyber posture trends in China, Russia, the United States and Theeuropean Union, Report*, Stockholm International Peace Research Institute, https://www.jstor.org, 2022, pp. 7-11. For more on CI information resilience, e.g. K.T. Kosmowski, *Towards strategic resilience of process plants and critical infrastructure regarding functional safety and cybersecurity requirements*, „Safety and Reliability of Systems and Processes", 2022, v. 3, pp. 117-132.

[5] The physical and cyber-physical systems necessary for the functioning of countries in the EU include, among others: energy and fuel supply; transport; banking; ICT networks; food production, processing and supply; water supply for the economy and citizens; health care; conditioning the continuity of state administration (Ł. Szewczyk, *Infrastruktura Krytyczna*, [in:] *Encyklopedia Bezpieczeństwa…*, pp. 621-622, 625).

[6] D. Juristic, *op.cit.*, pp. 1, 4.

CI sectors as well as the scale of the consequences of potential damage to, and/or paralysis of individual systems included in CI.

Activities in the area discussed also need to take into account individual CI levels (EU level; individual member states; regional level - if one exists at a particular point in time)[7]. Protection of CI against information threats[8] ought to take into consideration the diversity of systems being part of CI, and could be linked to other types of CI protection both at EU and member state level[9].

An important challenge is the selection of safeguards and methods for overseeing their operation in CI across the EU. This needs to take into account cost optimization, keeping CI in good working order as well as the private sector's significant presence in this segment of the economy[10].

The EU's policy on CI in the 20th and 21st centuries has been analysed on multiple occasions in the literature on the subject. As for the period after February 2022, key publications include an analysis of the effectiveness of EU Directive 2022/2555 (Directive NIS 2)[11]. Legal and organizational measures relating to CI information security have been more extensively discussed with Germany and the UK being used as examples[12]. Opportunities for transposing solutions adopted in the UE to other countries were studied[13], and selected aspects of cooperation between the EU and NATO on information security were examined[14].

---

[7] Ł. Szewczyk, *op.cit.*, p. 625.

[8] Legal, technical, physical, personal, ICT protection, among others. Extensively on threats and information barriers in Chapter 3 of the book: W. Fehler, *Podstawy bezpieczeństwa informacyjnego*, Siedlce 2021.

[10] Ł. Szewczyk, *op.cit.*, p. 622.

[10] W. Cendrowski, *Cyberbezpieczeństwo*, [in:] *Encyklopedia Bezpieczeństwa…*, p. 754.

[11] D.D.S. Ferguson, *The outcome efficacy of the entity risk management requirements of the NIS 2 Directive* "International Cybersecurity Law Review", 2023; V.Yu, Zubok, A.V. Davydiuk, T.M. Klymenko, *Cybersecurity of Critical Infrastructure in ukrainian legislation and in Directive (Eu) 2022/2555* „Electronic Modeling", 2023, vol. 45, pp. 54-66.

[12] S. Steiger, *Krieg im Cyberspace? Die militärische Nutzung des Netzes,* [in:] *Cybersicherheit in Innen- und Außenpolitik. Deutsche und britische Policies im Vergleich*, Hamburg 2022, pp. 223-256.

[13] А.Й. Жемба, О.О. Клюха, О.І. Качан, *Управління міжнародною політикою ЄС у сфері захисту критичної інфраструктури*. „Наукові Записки Національного - Університету «Острозькаакадемія».Серія «Економіка»", 2022, No 27, pp. 4–11.

[14] M. Brethous, N. Kovalčíková, *Next Level Partnership Bolstering EU-NATO cooperation to counter hybrid threats in the Western Balkans*, European Union Institute for Security Studies, https://www.jstor.org (01.12.2023).

This text includes an analysis of legislative acts and literature on the subject. The relevance of data analysis and synthesis is limited as researchers have not got access to many pieces of information about key CI information protection matters[15].

Situation prior to Russia's downright aggression

Given the reality described above, it is not surprising that since the beginning of the 21st century ensuring CI security has been at the forefront of efforts on the part of both EU authorities and individual member states[16].

Serious consideration was given to the possibility of information attacks[17] on CI systems and facilities. Awareness was raised realized to what extent the destruction of IC facilities would affect the security of citizens and, consequently, the countries' internal stability. For example, an EU directive which came into force in 2008 establishes a procedure for the identification and designation of European critical infrastructures (ECIs) and lays down the responsibilities of member states and private owners of such infrastructure[18].

In the UE in the 21st century coordination of CI security activities has grown in importance, not only between states[19] but also between public administration structures and entrepreneurs. Attempts have been made to develop transparent rules and procedures for relations between states, local governments and the owners of individual facilities.

Activities in that area were complicated by a significant number of economic, social or military issues associated with CI as well as the number of stakeholders interested in CI operation, both at EU level and individual member state level. Terrorist organizations came to be considered a major challenge – there was concern about the risk of simultaneous attacks on CI in individual EU member states both in cyberspace and the physical world.

---

[15] P. Swoboda, *Bezpieczeństwo informacji niejawnych*, [in:] *Encyklopedia Bezpieczeństwa*…, p. 316.

[16] S. Żurawski, Z. Ciekanowski, H. Wyrębek, *Zagrożenia infrastruktury krytycznej*, „Studia Administracji i Bezpieczeństwa", 2023, v. 13, p. 263.

[17] More on information attacks: P. Motylińska, *Atak informacyjny*, [in:] *Encyklopedia Bezpieczeństwa*…., pp. 172-177.

[18] Ł. Szewczyk, *op.cit.*, p. 624.

[19] A. Dziewulska, *Strategie bezpieczeństwa Unii Europejskiej*, „Studia Europejskie", 2016, v. 4, p. 38.

Threats posed by certain subjects of international law gradually grew. This was especially true of activities of hackers controlled by states. Other threats to CI information security were lower in importance. Examples include natural disasters (particularly floods, hurricanes, earthquakes, fires)[20]; offences other than one mentioned above, acts of vandalism or accidents. In the second decade of the 21st century, particularly since 2014, some EU member states, including Western European states, have had to defend themselves against "low-level state-sponsored cyberattacks"[21].

This served to centralize the EU's legal and organizational activities in this area[22]. Examples of such action include Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013[23]. A response to Russia's increased activity since 2014 included, amongst others, Information Security Directive (NIS Directive)[24] or (partially Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010[25]. In respect of the EU, the objective of particularly dangerous state-sponsored cyberattacks was to acquire offensive and defensive capabilities necessary for massive attacks on CI in EU member states in the future.

Even the COVID-19 pandemic did not change the situation. The biggest cyberattacks on Western countries' CI for which Russia is held responsible, include data theft in 2020, made possible by a security gap in SolarWinds Orion software and, in 2021, a cyberattack on Colonial Pipeline, which led to gasoline shortages in the East Coast of the US[26]. What was also important was simultaneous action by hackers controlled from China[27]. It forms a consistent whole with other aspects of China's

---

[20] R. Wódkiewicz, *op.cit.*, pp. 150-154, 156-157; M. Torbicki, D. Raith, *Safety of critical infrastructure exposed to operation and weather condition changes*, [in:] 15th Summer Safety & Reliability Seminars - SSARS 2021, 5-12 September 2021, pp. 339-350.

[21] S. Steiger, *op.cit.*, pp. 254, 261.

[22] L. Saalman, Fei Su, L.S. Dovgal, *op.cit.*, p. 21.

[23] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[24] Cf. L. Saalman, Fei Su, L.S. Dovgal, *op.cit.*, .p. 21.

[25] Its legal as well as energy security aspects are discussed by: K. Grzebiela: *Szczególne rozwiązania prawne w dziedzinie bezpieczeństwa energetycznego w sektorze gazu ziemnego adresowane do odbiorców chronionych paliw gazowych. Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego", 2023, v. 28, pp. 91-95.

[26] J. Scott, *Assessing Russia's role and responsibility in the Colonial Pipeline attack*, Atlantic Council, https://atlanticcouncil.org (21.12.2023).

[27] Extensive discussion of its context as exemplified by Sweden: G. Huskaj, J. Bengtsson, *The Manifestation of Chinese Strategies Into Offensive Cyberspace Opera-*

policy against CI in the EU28. As the EU's high representative for foreign affairs and security policy, J. Borrell said on the 14th of September 2020: "The Internet has also become an arena for geopolitical battles and the spread of disinformation. Some states are increasingly using it to limit civil liberties and advance their ideological goals"[29].

The EU's insufficient action against Russia's aggressive policy was due to divergences between EU member states[30]. In spite of that, serious consideration was given to a possibility of a future armed conflict starting with a cyberattack on CI targets[31]. In 2020 the necessity to review and modify the EU's cyber defence policy was emphasized. In July 2020 the EU unveiled a security strategy for the years 2020-2025. The document laid emphasis, amongst others, on the necessity to accord more attention to hybrid threats and to bolstering CI resilience in EU member states[32].

In mid-2021 hackers controlled by actors from the East intensified their attacks to gain access, inter alia, to EU countries' CI. Even more intense hacking activity was witnessed in early 2022.[33] Growing tension between the West and Russia caused the EU authorities to adopt, on the 15th of February 2022, *Roadmap on critical technologies for security and defence* [34]. On that same day, the following was adopted: *Proposal for a regulation of the European parliament and of the council establishing the Union Secure Connectivity Programme for the period 2023-2027*[35].

---

tions Targeting Sweden, Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021 A Virtual Conference Hosted By University of Chester UK 24th-25th June 2021, UK 2021, pp. 35-43.

[28] More on them: F. Jüris, *Security implications of China-owned critical infrastructure in the European Union*, European Union, https://op.europa.eu, June 2023 (15.12. 2023).

[29] J. Borrell, *Cyber diplomacy and shifting geopolitical landscapes*, European Union, https://europa.eu, 14.09.2020 (13.12.2023).

[30] A. Dziewulska, *European Security Strategies and the War in Ukraine*, „Studia Europejskie", 2023, vol. 2, pp. pp. 27-44.

[31] R. Kopeć, T. Wójtowicz, *Bitwa wieloobszarowa*, [w:] *Encyklopedia Bezpieczeństwa…*, p. 567.

[32] A. Czop, *Nowa Strategia Zwalczania Przestępczości zorganizowanej w UE*, [w:] *Encyklopedia Bezpieczeństwa…,* p. 519.

[33] J. Schröfl, *The War in the Ukraine: Uproar in cyber space - The Question of Information and Cyber Dominance*, „Österreichische Militärische Zeitschrift", 2023, p. 10.

[34] *Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the committee of the regions Roadmap on critical technologies for security and defence*, European Union, https://europa.eu (15.12.2023).

[35] *Proposal for a Regulation of the European Parliament and of The Council establishing the Union Secure Connectivity Programme for the period 2023-2027*, European Union, https://europa.eu (15.12.2023).

In the face of Russia's downright aggression against Ukraine

The consequences of Russia's aggression against Ukraine launched in February 2022, including the anticipated increase in attacks against CI[36] across the EU, instigated by Russia (and China), have made it necessary for the EU to take measures to enhance protection and resilience of CI facilities and networks.

Given the current scale and nature of confrontation between the West and Russia, it can be assumed that in the EU it is the broadly understood energy infrastructure[37] and weapons manufacturing and repair facilities as well as weapons and combat assets storage facilities that are especially in jeopardy. However, as Russia's policy against Ukraine shows, even dams are not immune to danger.

It is an accepted view that in cyberspace the West and Russia are not currently using their full capability to strike. They are afraid of severe retaliation if a total cyberattack campaign were to start[38]. Nevertheless, NATO[39] leadership's pressure to protect CI is an important factor that stimulates the EU's legal and organizational activities with regard to its CI. Other threats to CI security have not waned, either. For example, there are fears of Islamic terrorist attacks during the Olympic Games in in Paris[40]. At the same time, natural disasters linked to global warming have been growing in frequency and intensity[41].

---

[36] J. Schröfl, *op.cit.*, p. 14.

[37] More on EU's energy security in times of war, e.g.: І.В. Яковюк М.П. Цвеліх, *Енергетична безпека Європейського Союзу в умовах російської агресії проти України*, „Problems of Legality", 2023, v. 16, pp. 170-191.

[38] G.B. Mueller [et al.], *Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures*, pp. 11, 13-14, CSIS, https://www.csis.org (10.12.2023).

[39] *Vilnius Summit Communiqué, Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023*, NATO, https://www.nato.int; A.M. Dowd, C.R. Cook, *Bolstering Collective Resilience in Europe*, European Union Institute for Security Studies, https://www.jstor.org (13.12.2023); S. Czmur, *Infrastruktura krytyczna a odporność strategiczna państwa*, „Przegląd Komunikacyjny", 2023, no 5, pp. 26-27.

[40] *Francja ostrzega przed powrotem islamskiego terroryzmu do Europy przed igrzyskami olimpijskimi w Paryżu*, Bankier, https://www.bankier.pl (13.12.2023). More on current terrorist threats to CI: O. Heino, *Intelligent terrorism as a security threat to critical infrastructure*, „Security and Defence Quarterly", 2022, Vol. 39, No. 3, pp. 33-44.

[41] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, art. 13.

In March 2022 the EU Council approved "A Strategic Compass for Security and Defence"[42]. It was thought, among other things, that significant projects were necessary. In May 2022 "the EU Defence Innovation Scheme" (EUDIS) was launched. Steps were also taken to "identify and monitor risks associated with strategic dependencies (technologies and their associated value chains and actors, etc.)"[43]. There was realization of the magnitude of security challenges faced by the newly established Observatory of Critical Technologies[44]. Additional cybersecurity requirements for hardware and software were put forward in the European Commission's proposal referred to as "Cyber Resilience Act"[45]. On the 10th of November 2022 a report was published on progress of activities aiming at creating a synergy between the civil, defence and space industries.

In 2022 and 2023 the Network of National Coordination Centres and the European Cybersecurity Competence Centre[46] began operation. Of great importance for CI protection were new rules adopted by the European Parliament on the 14th of December 2022: the afore-mentioned legislative act, described in the literature on the subject Directive (EU) 2022/2555 of the European Parliament and of the Council, and Directive (EU) 2022/2557 of the European Parliament and of the Council. The latter directive entered into force on the 16th of January 2023.[47] It is intended to enhance CI resilience against all threats[48].

The directive emphasizes the need to streamline CI protection across the EU[49]. The legislative act provides a clearer and more complete description of CI and puts it into categories according to importance[50]. Articles 17 and 18 of the directive address a group of facilities that is narrow relative to CI. These are critical entities of particular EU signifi-

[42] *A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and security*, European Union, https://europa.eu (12.12.2023).

[43] *Commission Staff Working Document First progress report on the implementation of the Action Plan on synergies between civil, defence and space industries*, European Union, https://europa.eu (12.12.2023).

[44] *Ibidem*.

[45] *Proposal for a Regulation Of The European Parliament and Of The Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*, European Union, https://europa.eu (15.12.2023).

[46] *Commission Staff Working Document…*

[47] *Enhancing EU resilience: A step forward to identify critical entities for key sectors*, European Union, https://europa.eu (12.12.2023).

[48] Directive (EU) 2022/2557…, p. 3.

[49] *Ibidem*, art. 5.

[50] *Ibidem*, art. 6; D. Juristic, *op.cit.*, p. 3.

cance. The criterion applied was the provision of essential services, to or in, a minimum of 6 Member States[51].

The afore-mentioned directive 2022/2557 provides for more stringent requirements relating to risk assessments and the frequency thereof[52] as well as CI security reporting[53]. It was decided that, generally, entities managing individual facilities should submit a notification to state authorities no later than 24 hours after becoming aware of a serious (or potentially serious) incident or disruption in CI. Where a threat could affect six or more Member States, the European Commission must be notified of such an incident too[54].

Furthermore, entities managing individual CI facilities and/or systems should inform the public of attacks and disruptions where they determine that it "will be in the public interest to do so"[55]. That is why, for example, information about cyberattacks is disproportionately infrequently provided to the public, often in the form of aggregate statistical data.

In order to make it possible for information on the infrastructure discussed to be used for coordination of activities, the directive requires such information to be provided in appropriate format. This means, in particular, the possibility for information to be averaged by geographic area, by year, by sector or by subsector[56]. A key responsibility for the implementation of those obligations was assigned to state authorities as well as administration units and entities subordinate to the state authorities.

Individual member states have been given the right to establish more stringent regulations allowing the country concerned to achieve a higher level of resilience[57]. In Directive 2022/2557, the EU authorities emphasize that the list of CI facilities is a minimum one and individual member states can extend it where required[58]. The directive is also an attempt to establish legal conditions for better coordination of activities[59] and more effective control over CI facilities and systems[60]. In the wake of previous

[51] Directive (EU) 2022/2557…, art. 17, 18.

[52] *Ibidem.* Put briefly: in this case risk is defined as a combination of the scale of a potential loss or disruption caused by the incident and the probability of the occurrence of the threat.

[53] *Ibidem*,art. 8.

[54] *Ibidem*, art. 15.

[55] *Ibidem*, art. 15.

[56] *Ibidem*.

[57] *Ibidem*.

[58] *Ibidem*. List of these CI facilities at EU level was compiled in July 2023.

[59] *Ibidem*, art. 11.

[60] *Ibidem*.

legislation, the directive points out non-EU countries' involvement in the management of individual Union CI facilities (which is unfavourable for the EU's security)[61].

In the face of Russia's aggressive policy and the EU's strained relations with China, member states are expected to adopt national CI resilience strategies by the 17th of January 2026[62]. Such strategies ought to be updated at least once in four years[63]. This is expected, among other things, to take into consideration the tremendous pace of change in CI security.

National resilience strategies are expected, inter alia, to allow for a higher level of CI protection uniformization at EU level and, in a number of countries, for increased resilience[64], including thorough monitoring and appropriate response to hybrid attacks[65]. Directive 2022/2557 of the 14th of December 2022 provides that entities that manage CI facilities and systems may receive state assistance (including EU funds)[66]. Donald Ferguson emphasizes that "the effectiveness of risk management measures of the NIS 2 Directive is limited due to the narrow scope of the cybersecurity risk management measures"[67]. This is particularly true of measures focused on the reconnaissance phase of a cyberattack, as the EU authorities have placed emphasis on maintaining resilience of individual systems on a more general basis[68]. They presumably concluded that this was needed in view of the necessity to make allowances for significant costs of extending the range of measures that enhance CI resilience.

Great importance is attached to the implementation of Directive 2022/2557. To this end, guidelines contained in the afore-mentioned

[61] With decisions taken in 2022 and 2023 regarding CI facilities in the EU owned by enterprises controlled by Russia (e.g. in Italy, Germany or Bulgaria), that mainly concerned China's assets (F. Jüris, *op.cit.*).

[62] More on CI's place in EU states' national security strategies for CI until December 2022: P. Pătrașcu, *National Security Strategies and Critical Infrastructure: An Analysis of the European Union Member States*, „Romanian Military Thinking", 2022, v. 3, pp. 11-29.

[63] Directive (EU) 2022/2557…, art. 4.

[64] *Ibidem.*

[65] More on hybrid threats: amongst others O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Kraków 2017.

[66] Directive (EU) 2022/2557…, art. 10, art. 20.

[67] D.D.S. Ferguson, *op.cit.*. See: R. Kumar Jha, *Cyber-Physical Security Framework for Critical Infrastructure Protection in Power Systems*, ResearchGate, https://www.researchgate.net (20.12.2023).

[68] D.D.S. Ferguson, *op.cit.*, p. 14. See. A. Tomalska, *Preparing critical infrastructure for the future: Lessons learnt from the Covid-19 pandemic*, „Security and Defence Quarterly", 2022, v. 39 no 3, pp. 29-30.

Directive 300/2008 have been elaborated on. In addition to member states, responsibility for overseeing the implementation of the provisions was assigned to other entities. It is envisaged that special structures will be operating too: supervision structures, structures for communicating information between states as well as advisory structures[69]. Such structures would work, and exchange information, with their equivalents established pursuant to Directive 2022/2055[70]. The most important structure, of all the structures established under Directive 2022/2557, is the Critical Entities Resilience Group, set up in 2023 and operating at EU level[71]. Member states are expected to adopt secondary legislation for Directive 2022/2557 by the 17th of October 2024.[72] The degree of incorporation of Directive 2022/2557 into the laws of individual member states will be assessed by the European Commission by the 17th of July 2027. Starting from 2029, the European Commission will be submitting, to the European Parliament and the Council, reports on the operation and effectiveness as well as necessity of amendments, to Directive 2022/2557[73].

Despite organizational and legal efforts, over a perspective of several years, the current economic situation is significantly hampering efforts to increase, in real terms, funding for various aspects of CI protection in EU member states. What also complicates concerted action is the differences between member states in terms of economic situation. The growing amounts of public aid for the EU's private sector in 2022 and 2023 are likely to contribute indirectly to financial support for entities that manage CI facilities and networks[74].

Despite the difficult economic times, an important form of CI protection at EU level and in individual member states is the continuation of coordinated (and subsidized by the EU) extension of CI in areas with the so-called "bottlenecks". An example in point is the magnitude of the planned expansion of energy grids and the gas transmission network.

The sheer scale of action necessitated by the above legislative acts and projects, coupled with the fallibility of the systems used, costs of maintaining various alternative connections or backup supply systems, entail the necessity of committing more manpower and resources. This is

[69] Directive (EU) 2022/2557…, art. 13, art. 15, art. 18.

[70] *Ibidem*, art. 21.

[71] *Ibidem*, art. 13.

[72] *Ibidem*, art. 26.

[73] *Ibidem*, art. 25.

[74] *3-krotny wzrost roli państwowej pomocy publicznej dla przedsiębiorstw zagraża spójności jednolitego rynku*, Polski Instytut Ekonomiczny, https://pie.net.pl, 8.12.2023 (8.12.2023).

not an easy challenge given the current economic difficulties at EU level. It is no coincidence that Directive 2022/2557 emphasizes that measures taken to improve CI security must conform to the principle of necessity and proportionality of action[75].

In the face of increasing cyber espionage [76] and information warfare, it can be assumed that the importance of the army and of special forces in detecting threats to CI security has increased as well. This is exemplified by training for Poland's Territorial Defence Force soldiers in monitoring and protecting oil transmission infrastructure.

Another issue that hinders CI protection is the different dates when individual security measures for CI computer systems were put in place[77]. Varying levels of determination on the part of national governments are yet another factor that weakens the effectiveness of measures both at EU level and at lower CI levels. This refers both to the enforcement of regulations and individual countries' different approaches to social, technical and business requirements relating to CI protection[78]. Among other things, that is due to cultural differences including the degree to which procedures are complied with (e.g. differences in this respect between Germany and Greece).

Another challenge is constituted by different levels of the effectiveness of the machinery of government and intensity of corruption in individual EU member states (e.g. between Sweden and Bulgaria). What also matters is individual governments' assessment of threat posed by Russian and Chinese policies (Hungary is a case in point).

Further uniformization of standards and CI protection policies requires improving information exchange and interoperability at EU level. Given the confidentiality and sensitivity of the CI security policy, limited international cooperation is an unfavourable solution, as it gives rise to bureaucratic barriers. It reduces trust between key partners. It causes delays in data collection. As a result, it discourages coordination of activities[79]. The effectiveness of steps taken in the area discussed is also weakened by the degree of complexity of some of the CI systems. A case in point is the very important role, in the energy sector, of weather-contingent renewable energy sources whose significance is still increasing at fast pace.

---

[75] Directive (EU) 2022/2557…, art. 21.

[76] More on cyber espionage: A. Słota–Bohosiewicz, *Przeciwdziałanie cyberszpiegostwu w organizacji*, „Obronność. Zeszyty Naukowe", 2018, v. 4, pp. 302-305.

[77] D.D.S. Ferguson, *op.cit.*, p. 13 note 15.

[78] I. Leroy, I. Zolotaryova, *Critical infrastructure defense: perspectives from the EU and USA cyber experts*, „Visnyk Natsionalnoho Hirnychoho Universytetu", 2023, p. 169.

[79] G.B. Mueller [et al.], *op.cit.*, p. 15.

The afore-mentioned member states' different capabilities in terms of CI security are now effectively limited at EU level by "selection of effective, appropriate and proportionate measures as part of the risk management requirement and incident impact requirement"[80]. In reviewing the EU authorities' efforts, one must bear in mind the EU is dependent on CI that is installed outside its territory. For example, in early 2023, on a global basis, there were a total of 552 submarine cables (actual or proposed) with a length of almost 1,400 thousand km[81].

Conclusions

The current confrontation between the West and Russia in terms of CI security has produced the following results in the EU territory, inter alia:

- tightening of requirements with respect to: assessment of risk of attacks against CI and CI resilience reporting;
- significant unification and tightening of regulations;
- higher expenditures to strengthen CI resilience.

Important factors contributing to differences in legislative acts and organizational activities in respect of CI security include, inter alia:

- different levels of threat posed to CI by Russia in individual member states.
- different significance of individual countries in the current West – Russia confrontation.
- technological and cultural differences between individual EU member states.
- different economic potential of individual member states.
- varying levels of complexity of CI systems, coupled with their uneven distribution in the EU.

The attack on an underwater gas pipeline between Estonia and Finland in September 2023, carried out using conventional weapons, has increased the likelihood of heightened confrontation between the West and Russia in relation to CI security. It emphasizes the necessity to extend coordination of activities between EU member states and to support continued cooperation between state authority and private structures in the protection of CI. Collection of a larger volume of anonymized data, being part of such cooperation, will make it easier to capture trends

[80] Quoted from: D.D.S. Ferguson, *op.cit.*, p. 14.
[81] D. Juristic, *op.cit.*, p. 6; *Vilnius Summit Communiqué…*

shown by the attacks carried out[82]. Some of the researchers now claim that "in the coming period, more sophisticated threats such as man-made epidemics/pandemics, attacks with biological and chemical weapons, attacks from virtual space, and hybrid influence will be focused more and more on the vital infrastructures of society and the state, too"[83].

Bibliography

3-krotny wzrost roli państwowej pomocy publicznej dla przedsiębiorstw zagraża spójności jednolitego rynku, Polski Instytut Ekonomiczny, https://pie.net.pl, 8.12.2023 (8.12.2023).

A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and security European Union, https://europa.eu (12.12.2023).

Borrell J., *Cyber diplomacy and shifting geopolitical landscapes* European Union, https://europa.eu, 14.09.2020 (13.12.2023).

Brethous M., Kovalčíková N., *Next Level Partnership Bolstering EU-NATO cooperation to counter hybrid threats in the Western Balkans,* European Union Institute for Security Studies, https://www.jstor.org (01.12.2023).

Cendrowski W., *Cyberbezpieczeństwo*, [w:] *Encyklopedia Bezpieczeństwa*, eds O. Wasiuta, S. Wasiuta, v. 1, Kraków 2021.

Commission Staff Working Document First progress report on the implementation of the Action Plan on synergies between civil, defence and space industries, European Union, https://europa.eu (12.12.2023).

Czmur S., *Infrastruktura krytyczna a odporność strategiczna państwa*, „Przegląd Komunikacyjny", 2023, no 5.

Czop A., *Nowa Strategia Zwalczania Przestępczości zorganizowanej w UE,* eds O. Wasiuta, S. Wasiuta, v. 5, Kraków 2022.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

Dowd A.M., Cook C.R., *Bolstering Collective Resilience in Europe*, European Union Institute for Security Studies, https://www.jstor.org (13.12.2023).

Dziewulska A., *European Security Strategies and the War in Ukraine*, „Studia Europejskie", 2023, v. 2, no 41.

Dziewulska A., *Strategie bezpieczeństwa Unii Europejskiej*, „Studia Europejskie", 2016, v. 4.

Enhancing EU resilience: A step forward to identify critical entities for key sectors, European Union, https://europa.eu (12.12.2023).

[82] G.B. Mueller [et al.], *op.cit.*, p. 14.

[83] D. Jurisic, *op.cit.*, p. 1.

Falecki J., *Ochrona Infrastruktury Krytycznej*, [w:] *Encyklopedia Bezpieczeństwa*, eds O. Wasiuta, S. Wasiuta, v. 5, Kraków 2022.

Fehler W., *Podstawy bezpieczeństwa informacyjnego*, Siedlce 2021.

Ferguson D.D.S., *The outcome efficacy of the entity risk management requirements of the NIS 2 Directive*, "International Cybersecurity Law Review", 2023.

Grzebiela K., *Szczególne rozwiązania prawne w dziedzinie bezpieczeństwa energetycznego w sektorze gazu ziemnego adresowane do odbiorców chronionych paliw gazowych. Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego", 2023, v. 28.

Heino O., *Intelligent terrorism as a security threat to critical infrastructure*, „Security and Defence Quarterly", 2022, Vol. 39, No. 3.

Huskaj G., Bengtsson J., *The Manifestation of Chinese Strategies Into Offensive Cyberspace Operations Targeting Sweden*, Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021 A Virtual Conference Hosted By University of Chester UK 24th-25th June 2021, UK 2021.

Яковюк І.В., Цвеліх М.П., *Енергетична безпека Європейського Союзу в умовах російської агресії проти України*, „Problems of Legality", 2023, v. 16.

Jüris F., *Security implications of China-owned critical infrastructure in the European Union*, European Union, https://op.europa.eu, June 2023 (15.12.2023).

Juristic D., *Challenges of Critical Infrastructure protection in contemporary security environment*, [in:] *Security and crisis managementtheory and practice 9th International Scientific and Professional Conference 29.09.2023. and 30.09.2023*. ResearchGate, https://www.researchgate.net (01.12.2023).

Kopeć R., Wójtowicz T., *Bitwa wieloobszarowa*, [w:] *Encyklopedia Bezpieczeństwa*, eds O. Wasiuta, S. Wasiuta, v. 1, Kraków 2021.

Kosmowski K.T., *Towards strategic resilience of process plants and critical infrastructure regarding functional safety and cybersecurity requirements*, „Safety and Reliability of Systems and Processes", 2022, v. 3.

Kumar Jha R., *Cyber-Physical Security Framework for Critical Infrastructure Protection in Power Systems*, ResearchGate, https://www.researchgate.net (20.12.2023).

Leroy I., Zolotaryova I., *Critical infrastructure defense: perspectives from the EU and USA cyber experts*, „Visnyk Natsionalnoho Hirnychoho Universytetu", 2023.

Motylińska P., *Atak informacyjny*, [w:] *Encyklopedia Bezpieczeństwa*, eds O. Wasiuta, S. Wasiuta, v. 1, Kraków 2021.

Mueller G.B., [et al.], *Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures*, pp. 11, 13-14, CSIS, https://www.csis.org, 13.07.2023 (10.12.2023).

Pătrașcu P., *National Security Strategies and Critical Infrastructure: An Analysis of the European Union Member States*, „Romanian Military Thinking", 2022, v. 3.

Proposal for a Regulation of the European Parliament and of The Council establishing the Union Secure Connectivity Programme for the period 2023-2027, European Union, https://europa.eu (15.12.2023).

Proposal for a Regulation Of The European Parliament and Of The Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, European Union, https://europa.eu (15.12.2023).

Saalman, Fei Su, L.S. Dovgal, *Cyber posture trends in China, Russia, the United States and Theeuropean Union, Report*, Stockholm International Peace Research Institute, https://www.jstor.org, 2022 (15.12.2023).

Schröfl J., *The War in the Ukraine: Uproar in cyber space - The Question of Information and Cyber Dominance*, „Österreichische Militärische Zeitschrift", 2023.

Scott J., *Assessing Russia's role and responsibility in the Colonial Pipeline attack*, Atlantic Council, https://atlanticcouncil.org, 01.06.2020 (21.12.2023).

Słota-Bohosiewicz A., *Przeciwdziałanie cyberszpiegostwu w organizacji*, „Obronność. Zeszyty Naukowe", 2018, v. 4.

Steiger S., *Krieg im Cyberspace? Die militärische Nutzung des Netzes,* [in:] *Cybersicherheit in Innen- und Außenpolitik. Deutsche und britische Policies im Vergleich*, Hamburg 2022.

Swoboda P., *Bezpieczeństwo informacji niejawnych*, [w:] *Encyklopedia Bezpieczeństwa*, eds O. Wasiuta, S. Wasiuta, v. 1, Kraków 2021.

Szewczyk Ł., *Infrastruktura Krytyczna*, [w:] *Encyklopedia Bezpieczeństwa*, eds O. Wasiuta, S. Wasiuta, v. 2, Kraków 2021.

Tomalska A., *Preparing critical infrastructure for the future: Lessons learnt from the Covid-19 pandemic*, „Security and Defence Quarterly", 2022, v. 39, no 3.

Wasiuta O., Wasiuta S., *Wojna hybrydowa Rosji przeciwko Ukrainie*, Kraków 2017.

Wódkiewicz R., *Podstawowe zagrożenia funkcjonowania obiektów Infrastruktury Krytycznej*, „Zeszyty Naukowe SGSP", 2022, no 83.

Zubok V.Y., Davydiuk A.V., Klymenko T.M., *Cybersecurity of Critical Infrastructure in ukrainian legislation and in Directive (Eu) 2022/2555* „Electronic Modeling", 2023, no 45.

Żurawski S., Ciekanowski Z., Wyrębek H., *Zagrożenia infrastruktury krytycznej*, „Studia Administracji i Bezpieczeństwa", 2023, v. 13.

Жемба А.Й., О.О. Клюха, О.І. Качан, *Управління міжнародною політикою ЄС у сфері захисту критичної інфраструктури*. „Наукові Записки Національного Університету «Острозькаакадемія».Серія «Економіка»", 2022, No 27.

Prawne i organizacyjne aspekty przeciwdziałania zagrożeniom dla infrastruktury krytycznej UE po 24 lutego 2022 roku

Streszczenie

Z uwagi na znaczenie infrastruktury krytycznej troska o jej bezpieczeństwo zajmuje ważne miejsce w polityce UE. Obecna konfrontacja między Zachodem a Rosją pociągnęła za sobą na terenie UE znaczne zaostrzenie przepisów i wysokie nakłady zwiększające odporność IK w zakresie bezpieczeństwa informacyjnego. Mimo starań organizacyjnych i prawnych, w perspektywie średnioterminowej obecna sytuacja gospodarcza znacząco utrudnia utrzymanie wysokiego poziomu finansowania różnych aspektów ochrony IK w państwach członkowskich UE. Innym czynnikiem komplikującym efektywność działań w skali UE jest różny stopień determinacji władz państw w zakresie egzekwowania przepisów i innych działań w sferze ochrony IK. Jest m.in. związany z oceną przez władze danego państwa stopnia zagrożenia jakie stwarza polityka Rosji i Chin oraz różnym stopniem zagrożenia IK poszczególnych państw członkowskich atakiem ze strony Rosji. Wyzwanie stanowi także zróżnicowanie poziomu sprawności aparatu państwowego wewnątrz UE.

Słowa kluczowe: bezpieczeństwo informacyjne, infrastruktura krytyczna, Unia Europejska, konsekwencje agresji Rosji na Ukrainę w 2022 r.