Part V

CRITICAL INFRASTRUCTURE PROTECTION

Chapter 18

Selected Legal Aspects of National Security and Critical Infrastructure Protection in the European Union with Particular Reference to the Polish National Legislation

Grzegorz Ocieczek

Abstract

In the current geopolitical scenario, ensuring national security and the protection of critical infrastructure seem to be key elements for upholding the proper functioning of a state and, consequently, the safety of its citizens. This paper addresses issues related to the protection of critical infrastructure in territory of the European Union (EU). Particular attention is paid to issues regarding legal solutions to ensure the security of EU member states. EU directives concerning the immunity of critical entities (CER) and issues related to ensuring a high level of cybersecurity in the territory of the EU (NIS 2) are discussed. The paper is divided into several main parts, which, in addition to the above-mentioned issues regarding the legal aspects of critical infrastructure protection, also address security (e.g. types and divisions) and terrorism (e.g. the most important legal acts aimed at counteracting this very dangerous phenomenon is indicated). This study also discusses the European Security Strategy (2020–2025) and its most important objectives regarding the security of critical infrastructure, anti-terrorism, cybersecurity, and the protection of public spaces. Regarding national security, the paper discusses the various national security strategies from 1990 to the present in Poland, showing that the strategies pay

Grzegorz Ocieczek (2024) 'Selected Legal Aspects of National Security and Critical Infrastructure Protection in the European Union with Particular Reference to the Polish National Legislation'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 803–839. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_18

particular attention to the changing approaches to security, the assessment of the current situation at the time and threats involved, and the increasing need to ensure the protection of critical infrastructure. The publication ends with conclusions and postulates regarding the need to ensure national security and increase the protection of critical infrastructure.

Keywords: Critical infrastructure, national security, terrorism, cybersecurity, national security strategies, European security strategies.

1. Introduction: critical infrastructure

1.1. Concept and division of hazards

Directly related to the issue of security is the so-called negative definition of security or threat is directly related to security issues. According to the definition of the term "threat" in the Polish dictionary, 'a "threat" is a situation or condition that threatens someone or in which he or she feels threatened as well as someone who creates such a situation'.[1] According to Professor Kitler, a threat is defined as 'a state of mental consciousness caused by phenomena perceived as negative (dangerous), and at the same time it is a set of internal and (or) external circumstances that can cause a dangerous state for a given subject'.[2] In turn, Ficoń defined danger as: 'an event caused by fortuitous (natural) or non-fortuitous (intentional) causes, which has a negative impact on the functioning of a given system or causes adverse (dangerous) changes in its structure or functioning'.[3] Most authors propose what is known as the dichotomous division of hazards, namely, those caused independently of humans and those caused by humans.[4]

Certainly, the development of different categories of hazards is favoured by the development of civilisation, which can be considered an accelerator of phenomena that can be categorised as dangerous. With regard to the division of hazards, the following criteria for their emergence should be distinguished: the possibility of anticipation (e.g. controlled, forecastable, unpredictable); source of origin (e.g. natural, technical, social, civilisational, and/or environmental); type (e.g. small, medium, large); elimination time (e.g. short-, medium-, and long-term); causal determinism

[1] *Słownik Języka Polskiego PWN* [Dictionary of the Polish Language PWN], word: "security". [Online]. Available at: https://sjp.pwn.pl/slowniki/bezpieczeństwo (Accessed: 21 August 2022).

[2] Kitler, 2010, p. 52.

[3] Ficoń, 2007, p. 76.

[4] See, for example: Glen, 2011, p. 19 et seq.

(e.g. intentional, random, mixed). Another division of hazards is also proposed herein: spatial coverage (e.g. local, regional, national, international, and global); field of action (e.g. sectoral, religious, political, and universal); level of destruction (e.g. minimal, medium, and high total).[5]

Meanwhile, nonmilitary threats can take the form of natural hazards (e.g. natural disasters), risks associated with human activities (e.g. pollution, activities, ozone holes, and environmental predation), and risks of an extraordinary nature (e.g. accidents, disasters, riots, disruptions of all kinds in transport and energy).[6] Another typology of risks is as follows: (1) natural hazards (e.g. droughts, frosts, floods, fires, winds, earthquakes, avalanches, and precipitation); (2) military threats (e.g. by type of formation, by means of destruction); (3) social risks (e.g. social pathologies and mental disorders); (4) technical hazards (e.g. environmental, communication, technological, construction, municipal, and network emergencies).[7]

1.2. Critical infrastructure worldwide: focusing on the European Union

The concept of critical infrastructure describes that certain resources essential for the functioning of the state, as they provides services of strategic importance and, above all, necessary for daily life in the form of communication, transportation, energy, water, and health. Therefore, the destruction or damage to critical infrastructure can have irreversible consequences not only for the residents of the country in which the incident occurred but also for residents of neighbouring countries. The malfunction of critical infrastructure can additionally cause negative social and economic consequences.

Turning to the question of critical infrastructure, and in particular the need to protect it and ensure the security of the population living in a given territory, in ancient times critical infrastructure played a significant role in the functioning of the state. Examples include the irrigation facilities on the Nile, the grain storage facilities or the ports of Phoenicia, and the aqueducts in Rome. The proper functioning of critical infrastructure increases citizen security and the state of certainty. With regard to the protection of critical infrastructure, it becomes impossible not to mention the events in the world that have increased public awareness of this issue, and thus have been accelerators of actions to ensure its proper protection and security. On 13 and 14 July 1977, a power line failure in New York City left the city without electricity for two days. This event was followed by riots which resulted in the looting and destruction of 1,616 shops.[8] In addition to the aforementioned accidents, there is the major accident at the Fukushima nuclear power plant, which occurred as a result of the tsunami caused by the earthquake on 11 March 2011, off the

[5] Ficoń, 2007, p. 78.

[6] Mierzejewski, 2011, p. 48.

[7] Jakubczak, 2008, p. 402.

[8] Wadowski, 2018, p. 1237.

coast of Honshu Island. These events have resulted in an estimated 15.000–20.000 deaths.[9] The accident had a greater impact than the Chernobyl reactor accident on 26 April 1986, which was caused by operator errors.[10]

Mention should also be made of the massive attack on Estonia's critical infrastructure on 27 April 2007, when hackers affiliated with the Russian Federation are believed to have launched a massive attack that paralysed the country. After that evening, the wave of cyberattacks on the information technology (IT) infrastructure of the country only escalated, as the websites of the parliament, defence and justice ministries, political parties, the police, and even public schools were disabled. The cyberwar lasted for three weeks. During that time, after the initial surprise, a quickly-formed unit (Estonian Computer Emergency Response Team, also known as CERT-EE), led by Hillar Aarelaid, organized an improvised but ultimately effective defence until May 18, when the attacks abruptly stopped.[11] The most recent attacks on critical infrastructure took place in early March 2024 when the Asia-Africa-Europe 1, Europe India Gateway, Seacom, and TGN-Gulf cable networks were damaged. These attacks significantly hampered the passage through and around the Red Sea. The area has accounts for approximately 12% of maritime trade worldwide in recent years, and yet some ships are opting for longer circuitous routes because of the fear of repercussions.[12]

The first documents describing critical infrastructure protection issues were the 'Protocol Additional I to the Geneva Conventions of 12 August 1949', and the 'Protocol Additional II to the Geneva Conventions of 12 August 1949'. For example, Art. 55 of the Protocol Additional I deals with the protection of the environment, while its Art. 56 deals with the protection of structures and installations containing dangerous forces. According to para. 1 of Art. 56, structures and installations containing dangerous forces, particularly dams, dykes, and nuclear power stations, may not be subjected to attacks, even if they are military targets, as such attacks are likely to trigger such forces and consequently cause serious harm to the civilian population. Other military targets on or near such structures or facilities should not be subjected to attacks, as they are likely to trigger dangerous forces and consequently cause serious civilian casualties.[13]

In 1998, Bill Clinton issued a directive (named PDD-63) on critical infrastructure protection, the aim of which was to increase protection against possible terrorist attacks as well as the security of critical infrastructures. According to this document, critical infrastructure encompasses both physical and cyber-based system essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation,

[9] Jędrak, 2022; Wiech, 2021.

[10] *Katastrofa w Czarnobylu* [Chernobyl disaster], no date.

[11] Jalonen, 2009.

[12] *Incydent na Morzu Czerwonym. Kluczowe kable przecięte* [Incident on the Red Sea. Key cables cut], 2024.

[13] Art. 56(1) of the Protocol Additional to the Geneva Conventions of 12 August 1949.

water systems and emergency services, both governmental and private. Importantly, it was ordered that the state sector cooperate with the private sector to protect such critical infrastructure. According to the US Department of Homeland Security, approximately 85% of critical infrastructure remains in the private sector.[14] Immediately prior to this directive, on 15 July 1996, Executive Order 13010 was issued, based on which the President's Commission on Critical Infrastructure Protection was established. This Order also includes the definition of critical infrastructure, as follows:

> a structure of interdependent networks and systems comprising, identifiable industries, institutions (including people and procedures), and distribution capabilities that provide the flow of products and services essential to the defence and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.[15]

In the immediate aftermath of the terrorist attack on 11 September 2001, 27 pieces of legislation were enacted in the United States to intensify the protection of critical infrastructure.[16] One of the most important pieces was the Homeland Security Presidential Directive No. 7 of 17 December 2003, concerning the identification, priority, and protection of critical infrastructure of the state.[17]

Another important international document was the Council Directive of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection.[18] This Directive followed the adoption, on 20 October 2004, of Communication from the Commission on a European programme for critical infrastructure protection,[19] proposing ways to improve Europe's prevention of, preparedness for, and response to terrorist attacks against critical infrastructure. There was also the adoption of the Green Paper on a European Programme for Critical Infrastructure Protection (also known as EPCIP), which provided policy options for the development of the Programme and the Critical Infrastructure Warning Information Network. Art. 2a of the Directive defines critical infrastructure as a component, system, or part thereof, located in European Union (EU) Member States which is essential for the maintenance of vital societal functions, health, safety, security, material, or social well-being, and which

[14] Szewczyk and Pyznar, 2010, p. 53.

[15] Heniff, 2004, p. 5.

[16] Radvanovsky and McDougall, 2010, pp. 289–293.

[17] Tyburska, 2011, p. 147.

[18] *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. The previous document was: *The Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, of 12 December 2006*.

[19] *Green Paper on a European programme for critical infrastructure protection,* Para. 1, p. 2. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576 (Accessed: 21 August 2023).

would have a significant impact on a Member State in case disrupted or destroyed as a result of the loss of these functions. Art. 2b, in turn, defines the concept of European Critical Infrastructure (described as ECI), which refers to critical infrastructures located within the territory of Member States, the disruption or destruction of which would significantly affect two or more Member States. Whether the impact is significant is assessed with reference to crosscutting criteria, including impacts resulting from cross-sectoral interdependencies with other infrastructure.[20] The Directive also includes relevant considerations such as recognition of ECI, designation of ECI, protection plans, security liaison officers, and sensitive critical infrastructure protection information.

According to Annex 1 of the above Directive, the basic sectors to which critical infrastructure should be designated are the energy sector (e.g. electricity, oil, and gas) and the transport sector (e.g. road, rail, air, inland waterway, ocean shipping, short sea shipping, and ports).[21] Particularly important documents that have been published recently as part of the so-called Critical Infrastructure Protection regulatory package, which represents the latest developments on the issue, are as follows:

1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011;[22]
2. Directive on measures for a high common level of cybersecurity across the Union (NIS2) of 14 December 2022;[23]
3. Directive amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366, and (EU) 2016/2341 as regards digital operational resilience for the financial sector;[24]
4. 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.[25]

[20] Arts. 2a and 2b of *the Council Directive 2008/114/EC of 8 December 2008, on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.*

[21] *Annex No. 1, Council Directive 2008/114/EC of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.*

[22] *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.*

[23] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, on 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* (NIS 2 Directive).

[24] *Document 32022L2556, Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022, amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (Text with EEA relevance), PE/42/2022/REV/1.*

[25] *Critical Entity Resilience (CER) Directive of 27 December 2022.*

The implementation of the aforementioned legislation was primarily linked to the need for effective cyber security preparedness, as well as the range of risks emanating from it. Additionally, the COVID-19 pandemic and its negative impacts highlighted the need for a seamless supply chain.

The first piece of legislation, the Regulation of the European Parliament and of the Council (EU) on digital operational resilience for the financial sector, highlights issues related to information and communication technologies (ICTs) that support the complex systems used in day-to-day operations. According to point 1 of the Regulation,

> ICT keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole and the financial system more vulnerable to cyber threats or ICT disruptions.

This explains why the importance of the need to increase digital resilience, the definition of resilience standards, and the coordination of regulatory and supervisory work in this area. Another piece of legislation, the Directive on measures for a high common level of cyber-security within the Union (NIS2), calls in its sixth point for the extension of the scope of the rules by sector to the wider economy, so as to ensure that sectors and services essential for key social and economic activities in the internal market are comprehensively covered. In particular, this Directive seeks to address the shortcomings of the distinction between key service operators and digital service providers, as it has proven outdated by not reflecting the importance of the sectors or services concerned with social and economic activities in the internal market. In addition, the Directive sets a benchmark for cybersecurity risk management measures and incident reporting obligations in the sectors within its scope. Point 19 of the Directive further mentions that:

> Member States should be responsible for submitting to the Commission at least the number of essential and important entities for each sector and subsector referred to in the annexes, as well as relevant information about the number of identified entities and the provision, from among those laid down in this Directive, on the basis of which they were identified, and the type of service that they provide.

Regarding the issue of possible incidents, 'Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate incidents and risks' (point 41 of the Directive). Mutual international cooperation and coordination in preventing and restoring critical infrastructure and, most importantly, proper risk management are also important.

The Critical Entities Resilience Directive (CER) of 14 December 2022 repealing Council Directive 2008/114/EC, states in its first point that,

> Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy. It is therefore essential to set out a Union framework with the aim of both enhancing the resilience of critical entities in the internal market by laying down harmonised minimum rules and assisting them by means of coherent and dedicated support and supervision measures.

An important indication is provided by the recommendations described in point 43, according to which:

> As the objectives of this Directive cannot be sufficiently achieved by the Member States since they require harmonisation of requirements already contained in Directives. By reason of the scale and effects of the action, they can be better achieved at Union level. Action may be taken in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

The Directive amending Directives 2009/65/EC, et al. with regard to the operational digital resilience of the financial sector signals in its first point that:

> The Union needs to adequately and comprehensively address digital risks to all financial entities stemming from an increased use of information and communication technology (ICT) in the provision and consumption of financial services, thereby contributing to the realisation of the potential of digital finance, in terms of boosting innovation and promoting competition in a secure digital environment.

In accordance with Directive 2022/2557, there is no reduction in national laws, and the country can provide a higher level of resilience to critical actors. In addition, a strategy should be developed within 36 months to enhance the resilience of critical entities, and it is recommended that the Directive be updated every four years. Furthermore, it is important for EU Member States to conduct risk assessment, and the States have 36 months to identify critical entities. It is also important to indicate the criteria for determining the significance of the disruptive effect. Each country shall designate at least one authority responsible for national implementation and enforcement of the provisions set forth in this Directive. At the same time, EU Member States are required to support critical entities in enhancing their resilience through guidelines, methodologies, exercises, and training. In this regard, good cooperation among EU Member States in protecting critical infrastructure is necessary (Art. 7 of Directive 2022/2527). Under this Directive, critical entities must implement appropriate and proportionate technical, security, and organisational measures to ensure resilience. Critical entities, according to the relevant regulations, are given a tool to check the background of critical personnel in EU registries. In addition, the

European Commission may organise an advisory mission to assess the measures put in place by a critical entity to fulfil its obligations. Simultaneously, EU Member States shall ensure that European critical entities provide advisory missions with access to information, systems, and facilities related to the provision of critical services, as these necessary for the work of the advisory mission. Another important aspect is that EU Member States shall ensure that competent authorities have the power and means to carry out on-site inspections of the critical infrastructure, buildings, and premises used by the critical entity to provide critical services, and remotely monitor the critical entity's measures, as well as conduct or commission audits of critical entities.

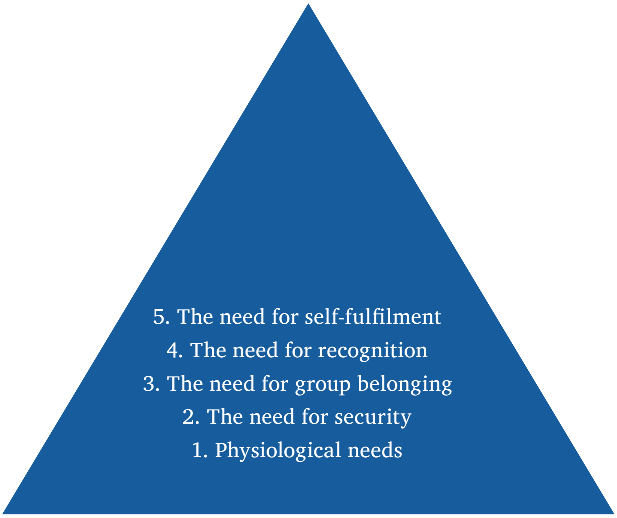
According to this all-important Directive, the critical entity should provide evidence of effective implementation of the measures, including the results of an audit conducted at the entity's expense by an independent and qualified auditor selected by the entity. Note that sanctions arise in the event of infringements of the national provisions adopted pursuant to this Directive, and these sanctions must be effective, proportional, and dissuasive. Only a properly functioning critical infrastructure can ensure proper economic development, which is why the aforementioned Directives and their proper implementation in the national system of individual EU Member States are important legal tools.

2. The concept of safety

Inextricably linked to the concept of critical infrastructure is security, the absence or weakening of which can adversely affect the operation of critical infrastructure. Security is a fundamental element in the functioning of a state and the life of its citizens. The civilisational development and scientific and technological progress seen in recent decades implies that, in theory, citizens should feel much safer. However, the development of modern technologies, especially in the field of information technology and the so-called digital space, can at the very least cause citizens to be concerned about excessive interference in their private lives. Additionally, and especially in light of the considerable social unrest and armed conflicts in Europe and across the world, a paradigm shift in security thinking has been observed in recent years.

Regarding the etymology of the term "security", it is derived from the Latin term "*sine cura*" (*securitas*), and according to the dictionary definition, security is considered to be the so-called 'state of not being threatened'. According to the Dictionary of National Security Terms, security is 'a state of affairs that provides a sense of certainty and guarantees for its preservation and a chance for improvement'. One of the basic human needs is a situation characterised by the absence of risk and of the possibility of loss of important things that a person particularly values, such as health, work, respect, feelings, and material goods.[26] Security is also defined as: 'the totality of conditions and institutions that protect the state and citizens from phenomena threatening the legal order', and as 'the protection of the system from attacks on the basic political institutions of the state'.[27] Maslow included the need for security in the second most important group of human needs, just after basic physiological needs. The following figure presents Maslow's pyramid of needs.

Figure 1. Maslow's pyramid


5. The need for self-fulfilment
4. The need for recognition
3. The need for group belonging
2. The need for security
1. Physiological needs

According to this author, 'If no need is satisfied, so that only physiological needs dominate in the organism, all other needs simply cease to exist or are relegated to the background'. Based on this argumentation, a question arises: is it the case that only after the basic needs have been satisfied, that is, physiological and safety needs, that other important needs appear?[28]

Still on the definition of the concept of security, it can be considered on three main levels, as follows: the ontological approach, related to the nature of security and where the basic element is the so-called existence and subjectivity; the epistemological approach, which attempts to identify the scientific cognition of the concept of "security" in its two dimensions (i.e. realistic and idealistic); the object-oriented approach, relating to the meaning of the term "security", which is framed in various sciences, including security sciences or defence sciences.[29] Security can also be con-

[26] Pawłowski, Zdrodowski and Kuliczkowski, 2020, p. 20 et seq.

[27] *Słownik Języka Polskiego PWN* [Dictionary of the Polish Language PWN], word: "security". [Online]. Available at: https://sjp.pwn.pl/słownik/bezpieczeństwo (Accessed: 27 July 2023).

[28] Maslow, 2006, pp. 63–68.

[29] Zdrodowski, 2019, pp. 48–50; See also: Brodie, 1949, p. 477; Zięba and Zając, 2010, p. 8.

sidered in relation to both its objective and subjective dimensions, the first being related to the objective state of the absence of physical danger.[30] Meanwhile, the subjective dimension relates to the state of consciousness of a certain subject/group, referring to a projection concerning the awareness of the perception of security. Security has also been described in terms of its internal security (i.e. the stability and harmony of a state) and external security (i.e. the absence of threats to the state and its citizens from external actors).[31]

2.1. Division of security

The concept of "security" is also interdisciplinary and transnational, and the Dictionary of Terms in the Field of National Security – developed by employees of the General Staff of the Polish Army, the Naval Academy, and the National Defence Academy based on literature presenting the views of doctrine representatives – systematises and presents a dozen of security concepts. Among the most important categories, there are the following:

- Global security, concerned with ensuring the security of all humanity and involving the major economic and military powers;
- Regional security, encompassing the security of countries in a particular region.
- National security, describing the survival of the state, including, inter alia, the freedom to pursue national interests.
- Military security, ensuring the ability to defend a given area and 'a state of awareness' in which the existing, projected, or possible level of military threat does not cause fear for the preservation of recognised values, the realisation of fundamental interests, and the achievement of strategic goals. This is based on the belief in the effectiveness of own and other actors' implemented and planned actions, and on the protective and defensive capabilities possessed.[32]
- Economic security, ensuring high efficiency in the development and functioning of the national economic system.
- Political security, consisting of activities related to the political dialogue conducted between countries and aimed at a country's security stability.
- Public security, referring to a status within the territory of a state made possible by efforts to provide organised protection and defence for persons and property against existing threats.
- Internal security, describing a state achieved by the actions of state bodies aimed at creating the most favourable international environment for a particular country, as well as strengthening its international position and image.

[30] Kołodziejczyk, 2007, p. 228.
[31] Zięba, 2001, pp. 217–219.
[32] Sadowski, 2015, p. 125.

- External security, consisting of the achievement of a state as a result of the actions of state bodies, aims to create the most favourable international environment for the country in question as well as to strengthen the country's international position and image.[33]

The concepts of international and national security are also noteworthy, the former being defined as follows,

> a state characterised by the absence of objectively existing threats and subjective concerns, and by the concerted efforts and actions of the international community to protect certain state and non-state (social) values by means of norms, institutions and instruments that ensure the peaceful settlement of disputes and the creation of economic, social, environmental and other prerequisites for dynamic stability and the elimination of threats". In turn, national security, identified with state security, is defined as "one of the basic areas of state functioning (activity) intended to enable the survival, but above all the development and freedom to pursue national interests in a specific security environment (conditions), by meeting challenges, exploiting opportunities, reducing risks and countering all kinds of threats to its interests.[34]

Therefore, security is, on the one hand, a continuous process, and, on the other hand, a status (i.e. associated with the absence of danger) that requires authorised bodies to ensure its maintenance.[35]

An important aspect concerning national security is the need to preserve its sovereignty and independence. The recent events related to the long-lasting, extremely expansive, and unauthorised foreign policy of the Russian Federation – as exemplified by the armed conflict in Georgia in 2008, the conflict in Ukraine in 2014 that resulted in the illegal annexation of Crimea, and the recent hostilities in Ukraine, showcase the importance of a country's internal security and the need to protect critical infrastructure. Significant for international security are also the recent developments related to the hostilities conducted between Palestine and Israel. Certainly, 2023 has brought about the need for a change in the approach of EU Member States, including Poland, to the perception of security, as well as the need for a remodelling based on the current situation beyond the EU's eastern borders and, in particular, the actions taken by the Russian Federation and Belarus. An important aspect in the area of security is the anti-terrorist measures taken by EU Member States, which in turn relate the intensification of threats of this kind.

At this point, mention should be made of the period of Poland's political transformation from to 1989/1990, when it was one of the first European countries to release itself from the influence of the Soviet Union, which started to effectively disintegrate

[33] Kaczmarek, Łepkowski and Zdrodowski, 2009, p. 14.

[34] Kaczmarek, Łepkowski and Zdrodowski, 2009, p. 25.

[35] Kukułka, 1995, p. 198 et seq.

on 16 November 1988, with the declaration of the sovereignty of Estonia. This disintegration process would see its ending only on 26 December 1991, when the Soviet Union passed a declaration of its self-dissolution. In Poland, its socio-political transition in the 1990s had a significant impact on its security issues, including those of an international nature. Authors dealing with these issues have pointed to the following as the main factors associated with the increase in crime and the decrease in security in the country: historical factors regarding the long-standing development of crime;[36] social factors, among which the dominant role was played by the collapse of values and authorities; a high level of acquiescence in the commission of certain types of crime, particularly of a fiscal and financial nature;[37] the public's demand for illegal services and goods that were previously unattainable for the average citizen.[38] Other factors were economic in nature and included structural and ownership changes, growing unemployment in a free market economy, increased crime in large cities (including criminal and tax crimes), and social stratification associated with the impoverishment of part of the population.

Meanwhile, the legal issues in Poland contributed to the inability to eliminate members of criminal groups, and some examples of these issues include the following: the failure to adapt its legal regulations to the prevailing market situation; the excessive liberalisation of laws, including those of a tax, criminal, economic, and procedural nature; the insufficient powers of law enforcement agencies to prevent crime and ensure an effective fight against it; the lack of effective methods to counter the intimidation of witnesses,. Other factors that associated with security issues in Poland were organisational/institutional factors, some of which were as follows: ineffective reform and reorganisation of law enforcement agencies,[39] which lacked sufficient competence and resources to combat members of organised crime group; cooperation of government officials (e.g. police, customs, tax authorities, and the UOP) with members of organised crime groups;[40] insufficient equipment and training of law enforcement officers, especially the for those in the police department;[41] lack of cooperation and coordination between services involved in combating crime.[42]

The international factors that influenced security issues in Poland resulted from, among other things, the points in the following list: the opening of the country's borders;[43] the socio-economic development in Europe;[44] the influx and penetration

[36] Ocieczek, 2023, pp. 75–101; Mądrzejowski, 2005, pp. 53–54.

[37] Sklepkowski and Woźniak, 1997, pp. 115–135.

[38] Kossowska, 2002, p. 588; Laskowska, 2011, p. 379; Hołyst, 2000, p. 312.

[39] An example of completely unjustified actions taken on the part of the management of the Ministry of the Interior and the KGP was the dissolution on April 6, 1990, of the Bureaus for Combating Economic Crime at the level of the KGP and the Provincial Headquarters of the Civic Militia. See: Rau, 2002, p. 53.

[40] Pływaczewski, 1992, pp. 39–40; Bagieński and Gontarczyk, 2013, p. 18 et seq.

[41] Pieprzny, 2007, p. 117.

[42] Laskowska, 2011, pp. 164–165.

[43] Hołyst, 2000, pp. 813–820.

[44] Pływaczewski, pp. 3–9.

of organised crime groups from Europe, especially from the former countries of the so-called Eastern Bloc;[45] population migration;[46] the collapse of the Soviet Union; the entry of Poland into the structures of the EU;[47] the lack of multilateral and bilateral international agreements;[48] deliberate actions on the part of Russian authorities, which made use of their special services (i.e. the Federal Security Service, also known as FSB, and Main Directorate of the General Staff of the Armed Forces of the Russian, also known as GRU) to attempt to destabilise the economic, political, and economic situation in Poland.

As can easily be seen, some of the factors described here still exist in some European countries today, which can cause mutual destabilisation, as least to some extent, on the international stage. At the beginning of the 1990s, the majority of the Polish population expressed concerns about their sense of security. Still, this situation seems to have improved significantly since 2000, when Poland became a full member of the North Atlantic Treaty Organization (NATO) and aspired for its membership in the EU. Meanwhile, the results of an Eurostat survey conducted with EU Member States shows that the problem of safety in large cities still exists in the United Kingdom (30.8%). Disturbingly, high results were also recorded for Bulgaria (25%), Germany (13%), Belgium (16%), the Netherlands (15%), Greece (12%), and France (15%). Thus, it seems that Poland's western neighbours, like the Belgians and the British, are facing lower levels of sense of security within large cities. Similarly, the Swedish government is considering amending legislation to protect citizens from organised crime. Furthermore, according to the 2023 Crime Index, the most dangerous cities in Europe were Bradford in the United Kingdom, Marseille in France, and Catania in Italy.[49]

2.2. Terrorism

This section concludes by discussing the issue of terrorism, which has evolved over recent decades along with technological progress and the adaptation to the prevailing geopolitical context. Although this subject will be explored in another separate study, it is worth mentioning certain aspects related to this phenomenon. The Polish legislation, in Art. 115 § 20 of the Penal Code, defines terrorist offences as being punishable by imprisonment of at least five years, and offences committed with the purpose of the serious intimidation of many people, forcing a public authority of the Republic of Poland or of another state or an authority of an international organisation to take or to refrain from taking certain actions, causing serious

[45] Gurov, 1990, p. 779 et seq; Gawenda, 2013, pp. 79–86; Rapacki, 2005; Świerczyński, 1997, pp. 187–198.

[46] Gałek, 2001, p. 71; Sklepkowski, 1997, pp. 155–175.

[47] Pływaczewski et al., 2011.

[48] Laskowska, 2006, p. 334.

[49] Europe: crime Index by City 2023. [Online]. Available at: https://www.numbeo.com/crime/region_rankings.jsp?title=2023&region=150 (Accessed: 4 October 2023).

disturbance to the system or economy of the Republic of Poland, another state or an international organisation, as well as the threat of such an act. Importantly, owing to the increasing terrorist threats, the Act of 10 June 2016 on Anti-Terrorist Activities[50] came into force on 2 July 2016, and according to the adopted assumptions,

> the basic aim of the regulation was to increase the effectiveness of the Polish anti-terrorist system, and thus increase the security of all citizens of the Republic of Poland, inter alia, through: strengthening the mechanisms for the coordination of activities, clarifying the tasks and areas of responsibility of individual services and bodies and the principles of cooperation between them, ensuring the possibility of effective action in the event of suspicion of an offence of a terrorist nature, including in the area of preparatory proceedings, ensuring response mechanisms adequate to the type of threats occurring and adapting criminal provisions to new types of terrorist activities.[51]

The Act introduced, among other things, a universally applicable and NATO-adapted four-level system of alert degrees for terrorist threats and cyberattacks. In addition, new types of terrorist offences were introduced, including, inter alia, the following: participation, for the purpose of committing a terrorist offence, in a training course that may enable the commission of such an offence (Art. 255a § 2 of the Penal Code); disseminating or publicly displaying content that may facilitate the commission of a terrorist offence, or for the purpose of gaining access to such content with the intent that such an offence be committed (Art. 255a § 1 of the Penal Code); setting up or leading an organised group or association with the aim of committing a terrorist offence (Art. 258 § 4 of the Penal Code). In the field of counterterrorism, important international legal acts normalising these issues include those outlined herein:

1. European Convention on the Suppression of Terrorism, drawn up on 27 January 1977, in Strasbourg;[52]
2. International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;[53]
3. International Convention Against the Taking of Hostages;[54]
4. Convention on the Physical Protection of Nuclear Material;[55]
5. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism;[56]

[50] *Act of 10 June 2016 on anti-terrorist activities*, 2016.

[51] *Ustawa o działaniach antyterrorystycznych* (omówienie) [The Act on Anti-Terrorism Measures (Overview)], no date.

[52] It entered into force on 4 August 1978, while Poland ratified the Convention on 30 January 1996 with effect from 1 May 1996.

[53] *International Convention for the Suppression of the Financing of Terrorism of 9 December 1999*, 1999.

[54] *International Convention Against the Taking of Hostages*, 1979.

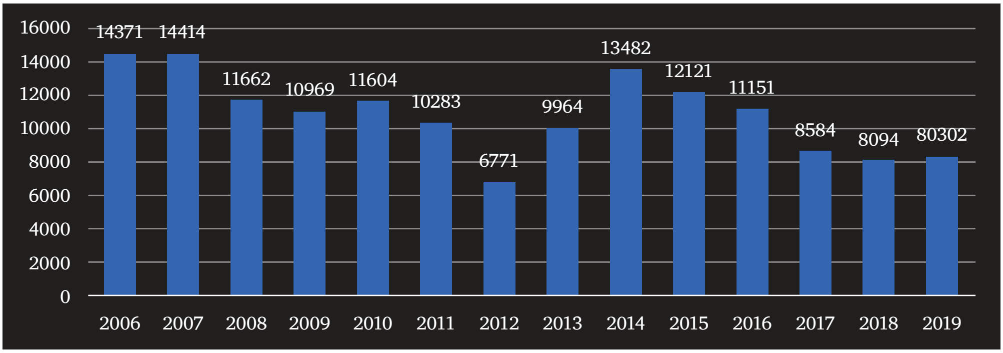
[55] *Convention on the Physical Protection of Nuclear Material*, 1979.

[56] *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)*, 2005.

6. Council of Europe Convention on the Prevention of Terrorism of 16 May 2005;[57]
7. International Convention for the Suppression of Terrorist Bombings;[58]
8. Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism of 22 October 2015;[59]
9. Council Decision (EU) 2018/889 of 4 June 2018, on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism;[60]
10. Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism.[61]

As is widely believed, 2001 became a watershed year for global terrorism in terms of, among other things, globalisation and reach, as that year saw one of the largest terrorist attacks in the history of the United States of America.[62] The chart below illustrates the number of terrorist attacks worldwide during 2006–2019.

Chart 1. Number of terrorist attacks worldwide during 2006–2019[63]



As can be seen, the reduction in terrorist attacks dates from 2011–2013, perhaps related to the elimination of the most notorious terrorist, Osama bin Laden, which took place on 2 May 2011. However, from 2014, when there was the annexation

[57] *Council of Europe Convention on the Prevention of Terrorism of 16 May 2005.*

[58] *International Convention for the Suppression of Terrorist Bombings*, 1997.

[59] *Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism*, 2015.

[60] *Council Decision (EU) 2018/889 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism.*

[61] *Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism.*

[62] Karolczak, 2022, p. 10.

[63] Author's numbers based on data in the following link: https://www.statista.com/statistics/202864/number-of-terrorist-attacks-world-wide/ (Accessed: 10 October 2023).

of Crimea by the Russian Federation authorities, and up until 2016, the number of terrorist attacks has definitely increased. It should be noted that the most active terrorist groups that carried out attacks worldwide in the years 2019 and 2020 were the Islamic State of Iraq and the Levant, the Taliban, Al-Shabaab, the Communist Party of India-Maoist, and Boko Haram.[64]

Similar to Poland, Hungary has also introduced changes to its anti-terrorism legislation. On 7 June 2016 the Hungarian parliament amended the constitution and revised several laws in response to terrorist threats. A terrorist emergency provision was also added to the Basic Law, which was introduced by the government and approved within 15 days by the parliament, with a two-thirds majority. This provision allows for the use of the national military for counterterrorism activities, and for the government to impose a curfew, restrictions on vehicle traffic, a ban on mass events, reinforce border protection, and secure tighter control of the Internet and postal communication. An Anti-Terrorism Information and Crime Analysis Centre (also known as TIBEK) was also established to collect and analyse data on public security threats.[65]

3. European Union Security Strategy (2020–2025)

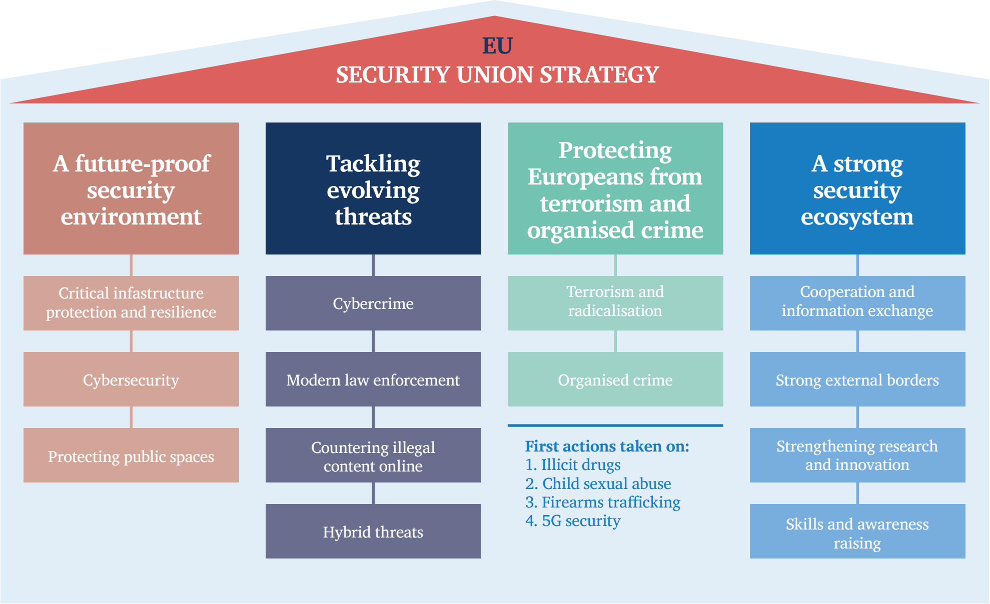
The European Security Union plays an important role in the security of the EU. This entity aims to ensure that EU security policy reflects changes in security threats in Europe, build long-term and sustainable resilience, and secure the involvement of EU institutions, agencies, governments, the private sector, and individuals in a whole-of-society approach. On 24 July 2020, the EU Security Strategy for 2020–2025 was published, the key pillars of which are the following:

- Focus on the fight against terrorism and organised crime, including organised crime, terrorism, and radicalisation.
- Provide a security environment that will stand the test of time and, in particular, tackle issues relating to critical infrastructure, cybersecurity, and public space protection.
- Build a strong safety ecosystem, including by improving research and innovation.
- Act in the face of changing threats such as hybrid threats, illegal content on the Internet, cybercrime, and modern law enforcement.[66]

The following diagram shows the most important elements of the Strategy.

[64] Dyvik, 2022.
[65] Sadecki, 2016.
[66] Balcewicz, 2020.

Chart 2. European Union Security Strategy Source[67]


EU
SECURITY UNION STRATEGY
A future-proof security environment
Critical infastructure protection and resilience
Cybersecurity
Protecting public spaces
Tackling evolving threats
Cybercrime
Modern law enforcement
Countering illegal content online
Hybrid threats
Protecting Europeans from terrorism and organised crime
Terrorism and radicalisation
Organised crime
First actions taken on:
1. Illicit drugs
2. Child sexual abuse
3. Firearms trafficking
4. 5G security
A strong security ecosystem
Cooperation and information exchange
Strong external borders
Strengthening research and innovation
Skills and awareness raising

On 13 December 2022 an interim report on the implementation of the EU Security Strategy was adopted. It emphasised that most of the strategy's tasks had been discussed, albeit achieving its full impact on security would require action to implement the agreed upon legal solutions in individual national legislations, including the NIS 2 Directive (i.e. strengthens security requirements, including on incident response and crisis management) and the CER Directive (i.e. covers the physical critical resilience of entities to man-made and natural hazards).[68] Within the framework of the aforementioned report, the sabotage of the Nord Stream gas pipeline and the resulting risks have received special attention. Importantly, and as further elaborated in the Critical Infrastructure Report, the NIS 2 Directive covers a wide range of sectors, including energy, transport, banking, finance, market infrastructure, banking, and health.

Important elements in the framework of the EU Security Strategy are the resilience of critical infrastructure and the creation of a legal framework capable of strengthening, both physically and digitally, such infrastructure. Therefore, public–private stakeholder cooperation for the proper maintenance of security seems crucial.

[67] Available at: https://cyberpolicy.nask.pl/strategia-bezpieczenstwa-ue-2020-2025/ (Accessed: 12 October 2023).

[68] *Communication from the Commission to the European Parliament and on the Fifth Progress Report on the implementation of the EU Security Union Strategy*, 2022.

4. National Security Strategies (1990–2020)

Another aspect, this time of a national nature, related to security – and which encompasses, inter alia, the protection of critical infrastructure – is the national security strategies prepared since 1990 in Poland, initially called the Defence Doctrine of the Republic of Poland. These documents play an exceptionally important role in the context of security issues within the EU and the NATO. These strategies are part of the framework of international security in Poland, considering a broad definition of the term. Still, the basis of this strategic planning has changed in Poland through the Act of 11 March 2022 on the defence of the homeland (that is, Thz. U. from 2024. 248). Currently, an olive-strategic Defence Directive of the Republic of Poland and other implementing documents are envisaged for the National Security Strategy.

This Strategy begins its history with the aforementioned socio-political changes. In 1990, for the first time, a document called the Defence Doctrine of the Republic of Poland was prepared. It was then adopted by a resolution of the Committee for the Defence of the Country on 21 February 1990, based on Art. 5(2)(1) and Art. 6 of the Act of 21 November 1967, on the Universal Obligation to Defend the People's Republic of Poland.[69] The Doctrine sets out directions for Poland's defence and security policies, and its basic premises set out that the purpose of creating this document was to 'guarantee the most vital interests of the Polish Nation: security, the right to live in peace, the independence and sovereignty of the state, and the integrity and inviolability of its territory'. In this document, particular attention was paid to geopolitical issues, particularly Poland's strategic location, as well as the need to build a Polish defence doctrine together with Western allies in order to secure the nation's territorial integrity. According to the second part of the document, Poland, in accordance with the Charter of the United Nations, undertook to renounce the use of force and the threat of its use in international relations, not to initiate hostilities against another state or an alliance of states, and not to participate in war on the condition that it or its allies do not become the object of an armed attack. Important aspects recognised in the Defence Doctrine were the need to develop mutual international guarantees and security obligations, the introduction of early warning systems, and the need to secure the efficient and rapid coordination of forces and measures with respect to existing threats, both during peacetime and in the event of war.

> The doctrine was the result of a kind of homework of a very belated lesson on state defence within an alliance (…) Firstly, the Warsaw Pact in 1990 was no longer an alliance, but a group of states calling themselves members of the Warsaw Pact, with practically no knowledge of any rules of joint action, and at the same time not

[69] *Act of 21 November 1967 on Universal Obligation to Defend the People's Republic of Poland, Journal of Laws.*

> knowing what to do in the new conditions. Secondly, a belated lesson, because there was no longer any chance to implement the solutions adopted.[70]

At the same time, the Defence Doctrine can be considered to having been developed during a transitional period, during which Poland launched a search for new solutions and a new approach, while at the same time trying to distance itself from the Warsaw Pact. According to General Koziej's controversial assessment, the operational tasks of the armed forces were not formulated very fortunately and were limited to defensive operations only; this was supposedly, in his words, related to the aftermath of the introduction of the Warsaw Pact War doctrine in 1987, which favoured a defensive character of operations. In the General's opinion, such an approach could have had negative consequences for the efficiency and effectiveness of the Polish armed forces.[71] This Doctrine that emerged during a period of socio-political transformation was a peculiar novelty for Poland, and was in line with its "relaxation" tendencies on the one hand, while it showed clear tendencies towards the construction of pan-European alliances in terms of ensuring national security on the other hand. The Defence Doctrine also covered the security system and described that it was responsible for several key areas of the country's functioning, including the protection of the military, political, social, administrative, and economic fields, as well as civil defence and state protection. However, this document did not consider issues concerning the protection of critical infrastructure.

Other documents directly related to security policy in Poland were those on the assumptions of the Polish security policy and the security policy and defence strategy of the Republic of Poland. The Polish National Defence Committee adopted these documents on 2 November 1992. Work on the Defence Doctrine was undertaken by an inter-ministerial team appointed by the President of the Republic of Poland on 5 August 1991 and organised at the Polish National Security Office. The assumptions of the Polish security policy were divided into six main segments, as follows: basic assumptions, integration with Western Europe, international security regime, new regional cooperation, and internal security. The basic assumptions described that:

the Republic of Poland treats its borders as inviolable and has no territorial claims on its neighbours. It respects the sovereignty of other states and renounces the use of force, including the threat of force, in bilateral relations with other states. Poland wishes to cooperate particularly closely with its neighbouring states.

A fundamental aspect of these assumptions regarding the integration of Poland with Western Europe was the question of Poland's future membership in the European Communities, which was important from the point of view of sovereignty and economic development. Regarding regional cooperation, attention was drawn to the need for Poland to develop cooperation with Hungary, the Czech Republic, and Slovakia. In connection with the social and economic changes occurring in Poland,

[70] Koziej and Brzozowski, 2015, p. 19.

[71] Koziej, 2008b.

particular attention was also paid to internal security, specifically regarding the transition to a free market economy, the rapidly growing crime rates, emigration, and environmental degradation. Security policymakers also did not lose sight of the range of threats that could arise from the so-called process of change in the East, or the radical regime transition. In terms of security aspects, attention was paid to the process of demilitarisation (disarmament), the creation of multinational armed forces, and the elimination of an atmosphere of military insecurity. According to the adopted strategy, the main factor for stability and security was being part of NATO, while the long-term factor and priority was to secure Poland's membership in the European Community.

Regarding the main assumptions about Poland's defence strategy, the document indicates the need to prepare, develop, and maintain the state's defence infrastructure, secure public defence preparedness, and make Polish armed forces ready to engage in defence and intervention activities in case of need. The concept of defence, in terms of the so-called non-military defence links, primarily concerned the protection of citizens against catastrophic industrial risks, natural disasters, and the effects of warfare. An important role of defence was also indicated to the National Civil Defence, as an extra-military defence link, as it was entrusted with the coordination of activities of all forces and means serving to protect the life and property of the population and cultural assets – within the framework of the state defence system. The powers of civil defence are also listed in detail, with some particularly noteworthy ones being described herein: planning undertakings for the protection of the life and health of the population; protecting workplaces, public utilities, and cultural assets from the effects of warfare; organising risk detection in this area; warning and alerting the population and its evacuation; preparing protective facilities; organising rescue and decontamination operations. The management of the state's defence was entrusted to the President of the Republic of Poland, the Prime Minister, and the Council of Ministers.

The above-mentioned basic tenets of the 1992 Security Strategy were different from those in the previous 1990 Defence Doctrine, at least with regard to possible threats. In this respect, there were no references to global conflicts in favour of local or regional conflict, and there was also a lot of space devoted to the socio–political transition, the disintegration of the Eastern Bloc, and the resulting possible tensions or destabilisation.

Finally, after many years of efforts by Poland – as the efforts started on 10 April 1992, during the first meeting of the NATO Military Committee, a recurring meeting that would eventually be attended by the Ministers of Defence and the Chiefs of Staff of Central and Eastern European countries on February 1999 – the President signed, with the prime minister's prior countersignature, the Act of Accession of the Republic of Poland to the North Atlantic Treaty.[72] During the political and economic transition period of Eastern Europe, especially after the collapse of the Soviet

[72] Dereń, 2016, pp. 17–30.

Union and the Warsaw Pact, the United States of America, with its great military and technological potential, played an important role in security policy. The United States of America regarded Europe as a strategic partner, while acknowledging that there was minimal security against armed conflict in Eastern European states. The result of this approach was the question as to whether the United States of America would assist countries such as Hungary, Poland, and the Czech Republic with their admission to NATO. Nonetheless, on 16 February 1995, the National Security Revitalization Act was passed in the House of Representatives of the U.S. Congress, which expanded NATO to include Poland, Hungary, the Czech Republic, and Slovakia. In Section 603 of US policy, item 1 indicated that the United States should continue its commitment to play an active leadership role in NATO. Point 2 of the resolution stated that, in terms of policy, it should join with the NATO allies in redefining the role of the alliance in the post-Cold War world, considering the following:

> (A) The fundamentally changed security environment in Central and Eastern Europe.
> (B) Need to reassure all states about the alliance's defensive nature and the desire of its members to cooperate with former adversaries.
> (C) Emerging security threats from the proliferation of nuclear, chemical, and biological weapons of mass destruction and their means of delivery.
> (D) Continued challenges to the interests of all NATO member states from unstable and undemocratic regimes with hostile intentions.
> E) Dependence of the global economy on stable energy supplies and free trade.

Regarding the participation of new partners, including Poland and Hungary, in accordance with Point 5 of the resolution:

> – that Poland, Hungary, the Czech Republic, and Slovakia should be in a position to further the principles of the North Atlantic Treaty and to contribute to the security of the North Atlantic area in the near future, and, in accordance with Article 10 of such Treaty, should be invited to become full NATO members, provided these countries---.
> (A) meet appropriate standards, including (…).[73]

The relevant document on Poland's security strategies following its accession to NATO was the Defence Strategy by the Council of Ministers, adopted on 23 May 2000. In terms of basic security policy objectives, the strategy included the following key topics: guarantee the independence, sovereignty, territorial integrity of the state and the inviolability of its borders; guarantee the protection of the democratic constitutional order, including, in particular, the fullness of rights and freedoms and the security of citizens of the Republic of Poland; create the best possible conditions for the comprehensive and stable social and economic development of the country, the well-being of its citizens, the preservation of the national heritage, and the development

[73] *H.R. 7 (104th): National Security Revitalization Act.*

of national identity; and contribute to the building of a lasting, just peace order in Europe and worldwide, based on the values of democracy, human rights, the rule of law, and solidarity. Regarding the conduct of security policy principles, the following came to the fore in this document: a comprehensive approach to national security issues; implementation of security policy with respect for the Polish Constitution and international law; a security policy guided, inter alia, by the values, ideals, and principles enshrined in the North Atlantic Treaty and the European Treaties in their actions on the international scene; the close link between national security and the security of NATO countries and EU Member States.[74] Similar to the previous security strategy, this strategy also emphasises the significant role of NATO and the issue of integration with the EU. In the sphere of defence operations, the above strategy distinguished between preventive and stabilisation actions, crisis response, and warfare, which should carried out in the event of possible aggression.

The 2003 National Security Strategy was adopted on 22 July 2003 and was signed by the President of the Republic of Poland on 8 September 2003. The need to develop and implement this new Strategy was connected with the outbreak of war in Iraq and the consequent participation of the Polish military, and with the issue of joining the structures of the EU in the near future.[75] The Strategy document begins with a chapter entitled "New Challenges", which presents the objectives of the state's policy and are unchangeable and concerned with maintaining the inviolability of borders and territorial integrity. This chapter emphasises Poland's participation in NATO and the guarantees associated with entry in EU structures. In the area of national threats, issues related to the so-called atypical threats, whose sources, often non-state actors, are difficult to identify, were signalled. The development processes in the field of ICT were also identified, as well as how they may entail certain threats, such as to the stability of the financial, capital, and economic situation of Poland. The general assumptions, which are described in the second chapter of the aforementioned document, point to the fact that the boundaries between the external and internal aspects of security were blurring at the time. Simultaneously, Poland committed to contributing to international security. The third chapter, titled "Tasks of state services", presents the need to continuously strengthen international relations with the United States of America, NATO, and the European Union. In the field of internal security, the issues of improving public safety through legislative changes, increasing the number of officers, changing the organisational structures of police, and ensuring the cooperation between the police and local authorities were signalled. Important issues such as the protection of ICT infrastructure and computer crime (novum) were not omitted. The fourth chapter, concerning the economic foundations of state security, discusses issues related to finance, budget, economy, infrastructure, environment, and education. With regard to critical infrastructure, it was assumed the following:

[74] *National Security Strategy of the Republic of Poland 2000*, p. 1.1.1 et seq.
[75] Lasoń, 2007, p. 57.

> efforts to maintain the proper condition of Polish infrastructure are one of the conditions for ensuring adequate defence potential and national security, both internal and external. In the coming years, it is necessary to increase the state's efforts to modernise the transport infrastructure, including the construction of motorways and expressways, sustainable development of railway transport, construction of airports and airstrips and the navigation system, changes in the structure and volume of transshipment of sea and inland shipping and land-sea transport and logistics chains. It will be necessary to intensify efforts to provide infrastructure on the eastern border of Poland, which will become the external border of the EU area.[76]

Both strategies do not sufficiently distinguish strategic and national interests. For obvious reasons, such as the war in Iraq, terrorist attacks in New York on 9 September 2001, and Poland's application to join EU structures, the issues of Poland's international activity were comprehensively described.[77] In addition, the tasks of the Polish armed forces were presented in a disorderly manner, and no holistic approach to the state security system was presented.[78]

In April 2007, another National Security Strategy of the Republic of Poland was adopted by the Council of Ministers. In the introduction, it reads as follows:

> '(…) the Republic of Poland is a safe country (…)'. It should be emphasised that since 1 May 2004 Poland has become a full member of the European Union structures, which certainly influenced the shape of the developed strategy. Moreover, it was emphasised that the National Security Strategy of the Republic of Poland, correlated with allied strategies, i.e. the NATO Strategic Concept and the European Security Strategy – constitutes the basis for the development of executive strategic directives, in particular the Political-Strategic Directive of the Republic of Poland, strategies of individual domains of national security, strategic plans of defence reaction and crisis management as well as long-term programmes of transformation of the state security system, including programmes of non-military defence preparations and programmes of development of the armed forces.[79]

The Strategy is divided into four main parts, which are devoted to such aspects as those outlined herein: national interests and strategic objectives of the Republic of Poland in the field of security; determinants of the national security of the Republic of Poland; the concept of national security; sectoral goals and objectives; the National Security System of the Republic of Poland. Regarding Poland's strategic objectives, the strategy referred to the common security interests of the countries centred around NATO and the EU. According to point 16, the main strategic objectives

[76] Koziej, 2008a.
[77] Trofimowicz-Kalinowska, no date, p. 145.
[78] Koziej and Brzozowski, 2015, pp. 32–34.
[79] *National Security Strategy of the Republic of Poland 2007*, Para. 5 of the Introduction.

included the following: ensuring the independence and territorial inviolability of the Republic of Poland and its sovereignty in deciding the internal affairs of the nation's life, its organisation, and the state system; creating conditions for civilisational and economic development; determining the capacity of the nation and the state to act; ensuring a sense of legal security for the citizens of the Republic of Poland.[80] Much attention has been paid to Poland's energy security in the context of the increasing threat of political exploitation of energy resources. The starting point in this respect, which dates to problems occurring in as early as 2007, was the need to ensure the diversification of supply and the use of alternative energy sources (Chapters 2.1, 2.2, and 3.6 of the Strategy). Other identified and indicated threat directions were terrorism, international crime (including organised crime), and threats of an environmental nature.

In the field of internal security, the strategy pays attention to the question of the ability to respond adequately to threats. The issue of critical infrastructure, both in terms of both development and protection, has not escaped attention. In this area, priority has been given to the need to develop a transport and communication infrastructure (Section 3.6, pt. 73) to ensure ecological security (Chapter 3.7) and IT and telecommunication security (Chapter 3.8). It should be acknowledged that this Strategy dealt with the system of national security in an exceptionally broad and detailed manner, paying attention to economic threats (e.g. in the field of raw material supplies and energy security).

On 5 November 2014, at the request of the Prime Minister, the President of the Republic of Poland approved the 2014 National Security Strategy of the Republic of Poland, which replaced the 2007 version. The 2014 National Security Strategy consisted of four main chapters, which were focused on the following: Poland as a security actor; security environment; strategic action concept and operational strategy; a strategic preparation concept with a preparation strategy. As rightly contested by Trofimowicz-Kalinowska '(…) the authors of the document (National Security Strategy of the Republic of Poland of 2014 r.) noted more challenges than threats, which indicates a positive assessment of Poland's security environment'.[81] Unfortunately, subsequent years have negatively verified the approach of the authors of this strategy in this regard, considering, for example, the extremely aggressive foreign policy of the Russian Federation, the armed conflict in Ukraine triggered by it (2014 sic!), and the migration crisis at the Polish–Belarusian border. An important aspect concerning this 2014 Security Strategy, as was the case in the 2007 Strategy, was the emphasis on Poland's membership in the Euro-Atlantic and European structures, which in turn determined the directions of both the threats and key fields of Poland's development. Regarding military cooperation, the United States of America once again occupied an important place, as did the desire to seek ties with countries such as Lithuania, Latvia, Estonia, Romania, and the Nordic Group. It was also

[80] *National Security Strategy of the Republic of Poland 2007,* Chapter 1.2 Point 16.

[81] Trofimowicz-Kalinowska, no date, p. 145 et seq.

emphasised that, in terms of security and relations with the Russian Federation, the so-called freedom to choose own development path, including its political and military alliances, should be guaranteed. The national interests outlined in the 2014 Strategy included the following:

> – To have an effective national security capability to ensure preparedness and capacity to prevent, including deter, defend, and protect against, as well as recover from, threats.
> – Individual and collective protection of citizens against threats to their life and health and against damage, loss, or degradation of their essential assets (tangible and intangible).
> – To ensure the free exercise of citizens' freedom and rights without detriment to the safety of others and the security of the state and to ensure national identity and cultural heritage.
> – To ensure the sustainable and balanced development of the country's social and economic potential, with particular attention to the protection of the natural environment and the living and health conditions of the population as the basis for living.

It is worth emphasising the factor indicated in the 2014 Strategy that is directly related to the protection of critical infrastructure, namely: 'ensuring the lasting and sustainable development of social potential and economic state, with particular emphasis on environmental protection natural environment and the living and health conditions of the population as the basis existence', which is described in Chapter I, Point 1.2. Examples of strategic objectives in the field of ensuring security, which are largely related to the protection of critical infrastructure, have been focused on, among other topics, the following in this document: maintaining and demonstrating the readiness of the integrated national security system to seize opportunities, address challenges, reduce risks and counter threats; improving and developing the national crisis management system to ensure its internal consistency and integrity, and to enable seamless cooperation within the crisis management systems of international organisations to which Poland is a member; protecting Poland's borders, which are the external border of the EU; protecting public order. Other important aspects were improving systemic solutions for preventing and combating terrorism and the proliferation of weapons of mass destruction; ensuring the safe functioning of the Republic of Poland in cyberspace and ensuring energy and climate security and the protection of the environment, biodiversity, and natural resources, especially water resources; shaping the country's spatial development in a way that increases resistance to a variety of threats, especially military, natural, and technological threats.[82]

Another element included in the security strategy was the protection of critical infrastructure. According to section 4.3(132) on the so-called protection subsystem,

[82] *National Security Strategy of the Republic of Poland 2014*, Chapter 1.2, Point 12.

> (…) The protection of the state's critical infrastructure requires structuring the legislation to create a single category of critical infrastructure facilities. This entails the need for changes in provisions for facilities subject to mandatory protection and those subject to special protection. Consistent legislation ensures that the resilience of all critical infrastructure elements is enhanced, which is the responsibility of a statutorily established critical infrastructure protection authority. New legislation should also create a system of real incentives for owners of critical infrastructure to invest in security.

This chapter defines the purpose of protection subsystems, which refer to the organisational, technical, and training development efforts related to the protection of the population, public order, and proper crisis management. In this respect, the role and key tasks of various institutions is outlined, as shown herein: justice; special services; bodies involved in countering and combating terrorism and extremism; authorities competent for cyber security; law enforcement services as well as critical infrastructure protection services; public safety services related to rescue and civil protection; border services; authority protection services and public administration.

In terms of strategic activities, chapter three of the Strategy presents priority directions for Poland, as follows: ensuring readiness and demonstrating determination to act in the sphere of security and defence; supporting processes to strengthen NATO's collective defence capabilities; developing the EU's Common Security and Defence Policy; strengthening strategic partnerships; supporting selective participation in the activities of the international community.[83] In summary, the 2014 National Security Strategy of the Republic of Poland, was a continuation and, in a way, a development of previous national strategies. However, some people criticised the way threats were presented, which, in their opinion, were too scattered throughout the strategy. In addition, as aforementioned, this strategy included more challenges than threats.[84]

At the request of the President of the Council of Ministers on 12 May 2020, the President of the Republic of Poland introduced a new National Security Strategy of the Republic of Poland, which replaced the 2014 Strategy. The main assumptions of this 2020 Strategy defined a comprehensive vision for shaping the national security of Poland in all dimensions. In addition, it considers the so-called subjective aspect, understood as the combination of the internal and international dimensions of security, as well as the physical aspect, considering all the dimensions of the functioning of the national security system. This strategy is in line with both the values described in the Constitution and the so-called context of Poland's presence in NATO and the EU.[85] The latest Security Strategy is divided into four key pillars, which are those described herein:

[83] *National Security Strategy of the Republic of Poland 2014*, Chapter III.

[84] Trofimowicz-Kalinowska, no date, p. 153.

[85] *National Security Strategy of the Republic of Poland 2020*, Warszawa, 2020. p. 9.

- Pillar I: Security of the state and citizens
- Pillar II: Poland's international security system
- Pillar III: National identity and heritage
- Pillar IV: Social and economic development, and environmental protection.

The description of the essential pillars of the strategy is preceded by an introduction, which discusses topics such as the security environment of values, national interests, and strategic objectives in the context of national security. With regard to the description of the security environment, the first problems addressed are the Russian Federation's pursuit of a neo-imperialist policy, which led to the illegal annexation of Crimea, aggression against Georgia, and unauthorised actions in eastern Ukraine. In addition, it is mentioned that the Russian Federation conducts activities below the threshold of war (of a hybrid nature) that carry the risk of creating conflicts (e.g. unintentional, resulting from a sudden escalation as a result of an incident, especially a military one), as well as comprehensive and complex actions by non-military means (e.g. cyberattacks and disinformation activities) with the aim of destabilising the structures of Western states and societies and cause divisions among allied states. Unfortunately, the last sentences of the strategy have been fully confirmed by the recent events that took place in Ukraine and the Moldovan region. In addition, the dangers arising from the development of new technologies, including digital technologies, and their creation of a dangerous space for the manipulation of information and disinformation, have been noted. Regarding Poland's critical infrastructure, such as power plants and transmission networks (especially electricity, gas, and gas storage networks), the Strategy noted that the development of oil and fuel transmission and storage networks to date was insufficient. The introductory part of the strategy also highlights issues concerning the need for Poland to be firmly embedded in transatlantic and European structures, and to develop bilateral and regional cooperation with key partners. The 2020 Strategy also addresses topics pertaining to financial security, economic stability, health protection, and safety threats in the area of environmental protection (Pillar IV, pp. 33–35).

In the 2020 Strategy, the national interests are defined by four key points, as follows: (1) guarding the independence, territorial integrity, sovereignty, and security of the state and its citizens; (2) shaping an international order based on solidarity, cooperation, and respect for international law, and providing guarantees for Poland's secure development; (3) strengthening the national identity and guarding the national heritage; (4) securing the conditions for sustainable and balanced social and economic development and environmental protection.[86]

The most elaborate of the Pillars of the 2020 Strategy is Pillar I, in which there are descriptions about national security management; state resilience and common defence; cybersecurity; information space. Particular attention should be paid to the second chapter of Pillar I, focused on increasing the state's resilience to threats

[86] *National Security Strategy of the Republic of Poland 2020*, Warszawa, 2020, p. 11.

through the creation of a system of universal defence, based on the efforts of the whole nation, and building an understanding of the development of the resilience and defence capabilities of the Republic of Poland. Section 2.8 draws attention to the need to implement a model for the protection of critical infrastructure, which in turn should be based on ensuring the continuity of its operation and services. Pillar II recommends, in the field of critical infrastructure, that the transport network should be developed to ensure an even saturation of infrastructure (especially in areas with limited transport accessibility to the TEN-T core) and a comprehensive network. These recommendations relate to the construction of the Polish section of the Via Carpatia, improvements in access to border crossings on the eastern border of the EU (Pillar II, Chapter II, Point 2.8), the expansion of seaports (Point 2.11), and the construction of the Central Communication Port and its inclusion in the national transport system (Point 2.13). With regard to the development of the aforementioned new technologies and the resulting threats, the 2020 Security Strategy recommends building the state's resilience to threats, including those of a hybrid nature, as well as enhancing its ability to protect the cybersphere. The suggestions for actions in this direction include conducting scientific research, continuously raising public awareness in this area, and obtaining the capability to conduct a full spectrum of military operations in the cyberspace. Pillar II of the 2020 National Security Strategy broadly coincides with the topics in the previous 2014 Strategy.

Pillar III should be regarded as the novel part of the Strategy, as its themes of identity and national heritage were addressed in a new way. This Pillar greatly focuses on strengthening the national identity, which is rooted in Christian heritage and universal values.

Pillar IV addresses the following topics: health and family protection; migration policy; economic security; energy security; environmental protection; scientific and technological potential. Regarding the protection of critical infrastructure, a particularly important issue presented in Pillar IV relates to energy security; this has become an important issue in light of recent events, particularly the aggressive war waged by the Russian Federation supported by Belarus against Ukraine, as it led to various economic sanctions being imposed by EU Member States on the Russian Federation. In accordance with Point 4, the key tasks of Poland are those outlined here: expand and modernise its energy generation capacity and electricity transmission and distribution networks to ensure continuity of supply (Point 4.1); increase the diversification of sources of crude oil and natural gas supplies (Point 4.2); increase the capacity, work safety, and range related to oil and fuel pipelines, as well as the capacity of fuel and oil depots (Point 4.3); continue the diplomatic, legal, and administrative activities aimed at stopping the construction of transmission infrastructure that increases the dependence of the Central European region on gas supplies from the Russian Federation (Point 4.4).

A very important provision of the 2020 Strategy from the perspective of state security is related to migration policy, which has become a significant problem in most EU Member States in recent years. Pillar IV, Point 2, describes the need:

> to develop and pursue a comprehensive migration policy, coordinated with the security, economic and social policy, taking into account both the current and projected needs of the labour market, integration of migrants into the Polish society, ensuring maintenance of social cohesion, as well as counteracting possible threats to public order and security related to migration processes.[87]

As far as national security strategies are concerned, one must agree that they should consider the assessment horizon – which should cover a period of five or six years and be shorter than one generation – and the assessment system – which should provide a general and specific view, and consider security-relevant opportunities, challenges, risks, and threats.

5. Conclusion

The security and protection of critical infrastructure in Poland are important issues and must be ensured, and this requires engaging in activities associated with ensuring physical, technical, personnel, ICT, and legal security. Specifically, it is key to draft and implement business continuity and restoration plans, referring here to sets of organisational and technical measures leading to the maintenance and (if necessary) restoration of functions performed by critical infrastructure.[88] Another important element in the protection of critical infrastructure is ensuring appropriate cooperation among Poland's institutions at the strategic, operational, and management levels, and at the international level. In terms of national regulations, important ones include those involved in ensuring a high common level of cybersecurity within the EU (NIS2; 14 December 2022), and the Critical Entity Resilience Directive (CER) (14 December 2022), which repealed Council Directive 2008/114/EC. The early detection of problems, resilience building efforts, and increasing citizens' awareness of the importance of securing the protection of critical infrastructure are also crucial steps toward securing the security of said infrastructure. Additionally, efforts should be made to develop research and thus use innovative solutions in this area.

As highlighted in the EU Security Strategy 2020–2025, it has become necessary, among other things, to do the following: adapt EU security systems to new threats; establish a joint cyber unit; improve law enforcement in the area of computer forensics as well as to counter hybrid threats. An extremely important aspect in the context of

[87] *National Security Strategy of the Republic of Poland 2020*, Warszawa, 2020, p. 32.

[88] *Resolution No. 210/2015 of the Council of Ministers of 2 November 2015, on the adoption of the National Programme for the Protection of Critical Infrastructure, with Annex No. 1 on standards to ensure the efficient functioning of critical infrastructure – good practices and recommendations.*

ensuring the security of critical infrastructure is also related to upholding its functionality, which may prove crucial in the face of the above man-made and natural threats. It should be emphasised that there is no “golden” means to guarantee the complete protection of critical infrastructure. Instead, such security is achieved by combining various elements, including the diversity of legal solutions in the field of critical infrastructure protection, engaging a significant number of entities responsible towards its protection and tackling an exceptionally large number of threats (i.e. natural and man-made). Therefore, only the introduction of ‘good practices’ in the field of critical infrastructure protection can bring the expected results in the form of minimising threats and ensuring the continuity of services and supplies of goods. An example of a ‘good practice’ is certainly the unification of law at the EU level and making efforts to promote international cooperation; for instance, joint training and exercises with other nations may contribute to ensuring appropriate immunity to critical infrastructure, improving related incident prevention, resilience, and timely recovery. Finally, it is worth mentioning that an extremely important aspect in the protection of critical infrastructure is ensuring legal security, which involves implementing appropriate security procedures, checking them, and systematically adapting them to real threats.

References

Bagieński, W., Gontarczyk, P. (2013) *Żelazo w dokumentach MSW i PZPR* [„Żelazo" scandal in the documents of the Ministry of Internal Affairs and the Polish United Workers' Party]. Warszawa: IPN.

Brodie, B. (1949) 'Strategy as a science', *World Politics*, 1(4), pp. 467–488; https://doi.org/10.2307/2008833.

Bryła, M. (2000) 'Porozumienie, zorganizowana grupa, związek przestępczy jako formy organizacyjne przestępczości zorganizowanej' [Agreement, organised group, criminal association as organisational forms of organised crime], *Prokuratura i Prawo*, 2000/3, pp. 24–39.

Dereń, J. (2016) 'Warszawski szczyt NATO projekcją sojuszniczego bezpieczeństwa' [The Warsaw NATO summit is a projection of allied security], *Rocznik Bezpieczeństwa Międzynarodowego*, 10(1), pp. 17–32.

Domański, Z. (2017) 'Bezpieczeństwo socjalne' [Social security], *Journal of Modern Science*, 2(33), pp. 367–384.

Ficoń, K. (2007) *Inżynieria zarzadzania kryzysowego. Podejście systemowe* [Engineering Crisis Management. A case-based approach]. Warszawa: Bell Studio Sp. z o. o., p. 76.

Gałek, D. (2001) 'Migracje legalne i nielegalne na wschodniej granicy RP' [Legal and illegal migrations on the eastern border of the Republic of Poland] in Białocerkiewicz, J. (ed.) *Wschodnia granica RP zewnętrzna granica Unii Europejskiej* [Eastern border of Poland External border of the European Union]. Kętrzyn: Materiały konferencyjne, p. 71.

Gawenda, A. (2013) 'Rosyjska przestępczość zorganizowana faktycznym zagrożeniem dla Polski' [Russian organised crime an actual threat to Poland], *Studia Prawnicze i Administracyjne*, 1(5), pp. 79–86.

Glen, A. (2011) 'Zagrożenia bezpieczeństwa narodowego RP' [Threats to the national security of the Republic of Poland] in Piątek, Z. (ed.) *Edukacja na rzecz bezpieczeństwa, Wybrane problemy* [Security education, Selected issues]. Warszawa: CSIEE.

Gurov, A. (1990) *Profiesyolalnaya priestupnost. Proshloye i sovriemiennost* [Professional crime. Past and present]. Moscow: Psihologičeskaja biblioteka.

Hołyst, B. (2000) *Kryminologia* [Criminology]. Warszawa: Wydawnictwo Prawnicze PWN, pp. 813–820.

Jakubczak, R. (ed.) (2008) *Obrona narodowa w tworzeniu bezpieczeństwa Polski w XXI wieku: podręcznik do przysposobieniu obronnego dla studentek i studentów* [National Defence in the Creation of Poland's Security the 21st Century: a textbook on defence preparation for students]. Warszawa: Dom Wydawniczy Bellon.

Kaczmarek, J., Łepkowski, W., Zdrodowski, B. (eds.) (2009) *Słownik terminow z zakresu bezpieczeństwa Narodowego* [Dictionary of national security terms]. Warszawa: Akademia Obrony Narodowej.

Karolczak, K. (2022) 'Terroryzm XXI wieku – wybrane aspekty' [Terrorism in the 21st century – selected aspects], *Terroryzm – studia, analizy, prewencja*, 1(1), pp. 9–28; https://doi.org/10.4467/27204383TER.22.001.15417.

Kitler, W. (2010) 'Bezpieczeństwo narodowe. Podstawowe kategorie, dylematy pojęciowe i próba systematyzacji' [National Security. Basic categories, conceptual dilemmas and an attempt at systematization], in Piekarski, M., Zdziech, M. (eds.) Warszawa: Zeszyty problemowe TWO, 1(61), p. 52.

Kołodziejczyk, A. (2007) 'Bezpieczeństwo jako fenomen społeczny: pojęcie bezpieczeństwa, jego interpretacje i odmiany' [Security as a social phenomenon: the concept of security, its interpretations and variations], *Seaculum Christianum: pismo historyczno-społeczne*, 14/1, pp. 223–252.

Kosewska, A. (1978) 'Przestępczość w wielkim mieście' [Crime in the big city] in Batwia, S., Jasiński, J. (eds.) *Zagadnienia nieprzystosowania społecznego i przestępczości w Polsce* [Issues of social maladjustment and crime in Poland]. Wrocław: Zakład Narodowy im. Ossolińskich.

Kossowska, A. (2002) 'Zapobieganie przestępczości w Polsce w latach 90 – perspektywa kryminologiczna' [Crime prevention in Poland in the 1990s – a criminological perspective] in Czapska, J., Kury, H. (eds.) *Mit represyjności albo o znaczeniu prewencji kryminalnej* [The myth of repressiveness or the importance of crime prevention]. Kraków: Wyższa Szkoła Bezpieczeństwa, pp. 585–603.

Koziej, S., Brzozowski, A. (2015) *Strategie Bezpieczeństwa Narodowego RP 1990-2014. Refleksja na ćwierćwiecze.* [The National Security Strategy of the Republic of Poland 1990-2014. Reflections for a quarter of a century]. Warszawa: Wojskowe Centrum Edukacji Obywatelkiej im. płk. dyplm. Mariana Porwita.

Kukułka, J. (1995) 'Nowe uwarunkowania i wymiary bezpieczeństwa międzynarodowego Polski' [New conditions and dimensions of Poland's international security], *Wieś i Państwo*, 1995/1, pp. 198–199.

Laskowska, K. (2006) *Rosyjskojęzyczna przestępczość zorganizowana. Studium kryminologiczne* [Russian-speaking Organized Crime. A criminological study]. Białystok: Temida 2.

Laskowska, K. (2011) *Etiologia przestępczości zorganizowanej w Polsce* [Etiology of organised crime in Poland]. Warszawa: C.H. Beck.

Lasoń, M. (2017) Polska strategia bezpieczeństwa narodowego na początku XXI wieku [Polish national security strategy at the beginning of the 21st century], *Krakowskie Studia Międzynarodowe*, 2007/4, pp. 49–63.

Maslow, A. (2006) *Motywacja i osobowość* [Motivation and Personality]. Warszawa: PWN.

Mądrzejowski, W. (2015) *Przestępczość zorganizowana. System zwalczania.* [The Scheme of Counteracting]. Warszawa: Editions Spotkania Spółka.

Mierzejewski, J. (2011) *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych* [European security under the impact of globalisation]. Toruń: Wydawnictwo Adam Marszałek.

Ocieczek, G. (2023) *Instytucja świadka koronnego w ujęciu materialnoprawnym, karnoprocesowym i empirycznym* [The institution of a crown witness in material legal, criminal procedural and empirical terms]. Warszawa: Wyawnictwo Instytutu Wymiaru Sprawiedliwości.

Pawłowski, J., Zdrodowski, B., Kuliczkowski, M. (2020) *Słownik terminów z zakresu bezpieczeństwa narodowego.* [Glossary of terms related to national security]. Toruń: Wydawnictwo Adam Marszałek.

Pieprzny, S. (2007) 'Zmiany prawno-organizacyjne w Policji w latach 1990-2007' [Legal and organisational changes in the Polish Police in 1990-2007] in Szymaniak, A., Ciepiela, W. (eds.) *Policja w Polsce. Stan obecny i perspektywy. Tom I.* [Police in Poland. Present state and perspectives. Vol. 1.]. Poznań: Wydawnictwo Naukowe Wydziału Nauk Politycznych i Dziennikarstwa UAM.

Pływaczewski, E. (1992) *Przestępczość Zorganizowana i jej zwalczanie w Europie Zachodniej (ze szczególnym uwzględnieniem republiki Federalnej Niemiec)* [Organised Crime and its Fight in Western Europe (with Particular Reference to the Federal Republic of Germany)]. Warszawa: Wydawnictwo Prawnicze.

Pływaczewski, E. (2011) *Przestępczość Zorganizowana* [Organized Crime]. Warszawa: C.H. Beck.

Radvanovsky, R., McDougall, A. (2010) *Critical Infrastructure. Homeland Security and Emergency Preparedness*. London, New York: CRC Press.

Rapacki, A. (2005) 'Przestępczość zorganizowana w Polsce – subiektywne spojrzenie policjanta' [Organised crime in Poland – a subjective view of a policeman], *Policja: kwartalnik kadry kierowniczej policji*, 2005/1.

Rau, Z. (2002) *Przestępczość zorganizowana w Polsce i jej zwalczanie* [Organised crime in Poland and its fight against it]. Kraków: Wolters Kluwer.

Sadowski, S. (2015) *Bezpieczeństwo militarne Rzeczpospolitej Polskiej* [The military security of the Republic of Poland]. Warszawa: Repozytorium UKW.

Sklepkowski, L., Woźniak, D. (1997) *Zorganizowana przestępczość gospodarcza w Polsce* [Organised economic crime in Poland] in Pływaczewski, E., Świerczewski, J., (eds.) *Policja polska wobec przestępczości* zorganizowanej [The Polish police against organised crime]. Szczytno: Wydawnictwo Wyższej Szkoły Policji, pp. 115–135.

Skrabacz, A. (2012) *Bezpieczeństwo społeczne – podstawy teoretyczne i praktyczne* [Social security – theoretical and practical foundations]. Warszawa: Dom Wydawniczy Elipsa.

Świerczyński J. (1997) *Przestępstwa popełniane w Polsce przez obywateli państw powstałych po upadku Związku Radzieckiego* [Crimes committed in Poland by citizens of countries established after the collapse of the Soviet Union] in Pływaczewski, W., Świerczewski, J. (eds.) *Policja Polska wobec przestępczości zorganizowanej* [Police of Poland against organised crime]. Szczytno: Wydawnictwo Wyższej Szkoły Policji, pp. 187–198.

Szewczyk, T., Pyznar, M. (2010) 'Ochrona infrastruktury krytycznej a zagrożenia asymetryczne' [Critical infrastructure protection and asymmetric threats], *Przegląd Bezpieczeństwa Wewnętrznego*, 2(2), pp. 53–59.

Tyburska, A. (2011) 'Policja a ochrona infrastruktury krytycznej' [Police and the protection of critical infrastructure], *Zeszyty Naukowe WSOWL*, 3(161), pp. 143–162; https://doi.org/10.5604/01.3001.0002.3052.

Wadowski, J.S. (2018) 'Ochrona infrastruktury krytycznej. Geneza problemu' [Critical infrastructure protection. Genesis of the problem], *Organizacja i zarządzanie*, 2018/6, pp. 1237–1241.

Zdrodowski, B. (2019) 'Istota bezpieczeństwa państwa' [The essence of national security], *Annales Universitatis Pedagogicae Cracoviensis: Studia de Securitate*, 9(3), pp. 47–71.

Zięba R. (2001) *Instytucjonalizacja bezpieczeństwa europejskiego* [Institutionalisation of European security]. Warszawa: Wydawnictwo Naukowe Scholar.

Zięba, R., Zając, J. (2010) *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski* [Building an integrated system of national security for Poland]. Warszawa: Ministerstwo Rozwoju Regionalnego.

Zybertowicz, A. (2005) 'AntyRozwojowe Grupy Interesów: zarys analizy' [Anti-Development Interest Groups: outline of analysis] in Wesołowski, W., Włodarek, J. (eds.) *Kręgi integracji i rodzaje tożsamości [Integration circles and types of identity]*. Wydawnictwo Naukowe Scholar: Warszawa, pp. 1–22.

Legislation

Act of 21 November 1967 on Universal Obligation to Defend the People's Republic of Poland (1967) Journal of Laws, 1988, No. 30, item 207, as amended.

Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2015) Official Journal of European Union, L 159/17, Ryga, 22 June 2015.

Annex No. 1, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008) Official Journal of the European Union, L 345/75, 23 December 2008.

Convention on the Physical Protection of Nuclear Material (1979) Vienna, 26 October 1979.

Council Decision (EU) 2018/889 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism (2018) Official Journal of the European Union, L 159, 22 June 2018.

Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2018) Official Journal of the European Union, L 159, 22 June 2018.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008) Official Journal of the European Union, L 345/75, 23 December 2008.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198) (2005) Warsaw, 16 May 2005.

Council of Europe Convention on the Prevention of Terrorism (2005) Official Journal of the European Union, L 159/3, Warsaw, 16 May 2015.

Critical Entity Resilience (CER) Directive of 27 December 2022 (2022) Official Journal of the European Union, L 333/164, 27 December 2022.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on 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 (NIS 2 Directive) (2022) Official Journal of the European Union, L 333/80, 27 December 2022.

Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022, amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (Text with EEA relevance), PE/42/2022/REV/1 (2022) Official Journal of the European Union, 27 December 2022.

H.R. 7 (104th): National Security Revitalization Act.

International Convention Against the Taking of Hostages (1979) New York, 17 December 1979.

International Convention for the Suppression of Terrorist Bombings (1997) New York, 15 December 1997.

International Convention for the Suppression of the Financing of Terrorism (1999) OJ. 263, items 2619 and 2620, New York, 9 December 1999.

National Security Strategy of the Republic of Poland 2000.

Protocol Additional to the Geneva Conventions of 12 August 1949.

Regulation (EU) 2022/2554 of the European Parliament and of the Counsil of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, (2022) OJ EU L 333/1, 27 December 2022.

Resolution No. 210/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure with Annex No. 1 on standards to ensure the efficient functioning of critical infrastructure – good practices and recommendations.

Weekly Copilation of Presidential Documents. US Government Printing Office. Washington DC.20402/ No. 3/ Vol. 29/ January, 25/ 1993.

Intermedia

Act of 10 June 2016 on anti-terrorist activities (2016) Journal of Laws 2016, item 904. [Online]. Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20160000904 (Accessed: 9 October 2023).

Balcewicz, J. (2020) 'Strategia Bezpieczeństwa UE 2020-2025' [EU Security Strategy for 2020–2025], *Cyber Policy*, 21 August 2020. [Online]. Available at: https://cyberpolicy.nask.pl/strategia-bezpieczenstwa-ue-2020-2025/ (Accessed: 12 October 2023).

Dyvik, E.H. (2022) 'Most active terrorist organizations worldwide in 2020, by number of attacks', *Statista*, July 2022. [Online]. Available at: https://www.statista.com/statistics/937553/terrorism-most-active-perpetrator-group-worldwide (Accessed: 10 October 2023).

Europe: crime Index by City 2023 (2023) *Numbeo*. [Online]. Available at: https://www.numbeo.com/crime/region_rankings.jsp?title=2023&region=150 (Accessed: 4 October 2023).

Green Paper on a European programme for critical infrastructure protection, Commission of the European Communities (2005) COM(2005) 576 final, Brussels, 17 November 2005. [Online]. Available at: http://eurex.europa.eu/LexUriServ/site/pl/com/ (Accessed: 21 August 2023).

Incydent na Morzu Czerwonym. Kluczowe kable przecięte [Incident on the Red Sea. Key cables cut] (2024) *Polsat News*, 5 March 2024. [Online]. Available at: https://www.polsatnews.pl/wiadomosc/2024-03-05/incydent-na-morzu-czerwonym-kluczowe-kable-przeciete/ (Accessed: 10 March 2024).

Jalonen, J. (2009) 'Dni, które wstrząsnęły Estonią' [The days that shook Estonia], *Eesti*, 12 May 2009. [Online]. Available at: www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (Accessed: 21 August 2023).

Jędrak, J. (2022) 'Ile ofiar pochłonęła katastrofa w Fukushimie? Tysiące, ale z nieoczywistego powodu' [How many lives were claimed by the Fukushima disaster? Thousands, but for an unobvious reason], *smogLab*, 11 March 2022. [Online]. Available at: https://smoglab.pl/fukushima-ofiary-wplyw-na-srodowisko (Accessed: 24 August 2023).

Katastrofa w Czarnobylu [Chernobyl Disaster] (no date) *Centralne Biuro Antykorupcyjne*. [Online]. Available at: https://antykorupcja.gov.pl/ak/retrospekcje/retro/6351,Katastrofa-w-Czarnobylu.html (Accessed: 24 August 2023).

Koziej, S. (2008a) *Strategie Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2003 i 2007 roku. Skrypt internetowy* [National Security Strategies of the Republic of Poland of 2003 and 2007], Warszawa: Skrytp Internetowy. [Online]. Available at: https://koziej.pl/publikacje/ (Accessed: 3 August 2023).

Koziej, S. (2008b) *Ewolucja bezpieczeństwa narodowego rzeczpospolitej Polskiej w latach dziewięćdziesiątych XX wieku. Skrypt internetowy* [Evolution of national security of the Republic of Poland in the 1990s.]. Warszawa: Skrypt Internetowy. [Online]. Available at: https://www.koziej.pl (Accessed: 3 August 2023).

Kuczabski, M. (2021) *Bezpieczeństwo psychiczne jednostki jako podstawa humanistycznego podejścia do bezpieczeństwa narodowego* [Psychological security of the individual as the basis of a humanistic approach to national security]. [Online]. Available at: https://www.researchgate.net/publication/354386492_Mental_security_of_an_individual_as_the_basis_of_a_humanistic_approach_to_national_security (Accessed: 2 August 2023).

National Security Strategy of the Republic of Poland 2003 (2003) Warsaw: Ministry of National Defence of Poland. [Online]. Available at: https://dataspace.princeton.edu/handle/88435/dsp016m311r75x (Accessed: 10 October 2023).

National Security Strategy of the Republic of Poland 2007 (2007) Warsaw: Ministry of National Defence of Poland. [Online]. Available at: https://dataspace.princeton.edu/handle/88435/dsp01g445cg59q (Accessed: 10 October 2023).

National Security Strategy of the Republic of Poland 2014 (2014) Warsaw: Biuro Bezpieczeństwa Narodowego. [Online]. Available at: https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf (Accessed: 10 October 2023).

National Security Strategy of the Republic of Poland 2020 (2020) Warsaw: Biuro Bezpieczeństwa Narodowego. [Online]. Available at: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf (Accessed: 10 October 2023).

Sadecki, A. (2016) ‘Pakiet antyterrorystyczny na Węgrzech’ [Anti-terrorist package in Hungary], *Ośrodek Studiów Wschodnich*, 15 June 2016. [Online]. Available at: https://www.osw.waw.pl/pl/publikacje/analizy/2016-06-15/pakiet-antyterrorystyczny-na-wegrzech (Accessed: 10 October 2023).

Słownik Języka Polskiego PWN [Dictionary of the Polish Language PWN]. [Online]. Available at: https://sjp.pwn.pl (Accessed: 21 August 2023).

Trofimowicz-Kalinowska, K. (no date) *Pojęcie bezpieczeństwa w strategii bezpieczeństwa narodowego Polski i Hiszpanii* [The concept of security in the National Security Strategy of Poland and Spain]. Core. [Online]. Available at: https://core.ac.uk/download/pdf/187227208.pdf (Accessed: 17 August 2023).

Wiech, J. (2021) ‘Fukushima minuta po minucie. Co się stało w japońskiej elektrowni jądrowej’ [Fukushima minute by minute. What happened at Japan’s nuclear power plant], *Energetyka 24*, 11 March 2021. [Online]. Available at: https://energetyka24.com/atom/fukushima-minuta-po-minucie-co-sie-stalo-w-japonskiej-elektrowni-jadrowej (Accessed: 24 August 2023).

Reports and communication

Raport Rządowy RP skierowany do Sejmu RP (2000) ‘Bezpieczeństwo i porządek publiczny’ [Government Report to the Sejm of the Republic of Poland, Security and Public Order], Warszawa, 13 June 2000.

Heniff, B. (2004) ‘CRS Report for Congress: Congressional Budget Action in 2004’, *Congressional Research Service*, 27 December 2004.

Communication from the Commission to the European Parliament and the on the Fifth Progress Report on the implementation of the EU Security Union Strategy (2022) COM(2022) 745 final, Brussels, 13 December 2022.