European Integration Studies, Volume 20, Number 2 (2024), pp. 319-343.
https://doi.org/10.46941/2024.2.13

GRZEGORZ OCIECZEK*

The Internal Security Agency and Poland's Critical Infrastructure Protection: Challenges and Solutions**

ABSTRACT: This article is devoted to critical infrastructure protection issues, with a focus on national regulations. It does not omit issues concerning the authorities which, according to the regulations, are responsible for critical infrastructure protection, including: relevant ministers, the Government Security Centre as well as the Internal Security Agency. The publication also presents issues related to ensuring information and communication technology security and countering terrorist threats, espionage and cyber-attacks. The empirical aspect of citing an excerpt from a research on terrorism, which was conducted in 2022 by ABW officers among representatives of academia as well as representatives of services and institutions belonging to the anti-terrorism community involved in terrorism studies, has not been disregarded either. The research points to a growing threat to the European Union from terrorist attacks. The article concludes with postulates on the need to increase the protection of critical infrastructure, in particular through proper risk assessment, as well as the need to develop an IT model for threat knowledge management.

Keywords: critical infrastructure, terrorism, cyber-terrorism, crisis management, Internal Security Agency.

*Assistant professor, Faculty of Law in the Department of Criminal Procedure, UKSW, Warsaw, Poland. https://orcid.org/0000-0002-2785-4677, g.ocieczek@uksw.edu.pl.

** The research and preparation of this study was supported by the Central European Academy.

1. National critical infrastructure

Critical infrastructure plays an extremely important role in this day and age, especially in the current socio-economic context. Its protection is of particular importance given the recent events beyond Poland's eastern border in connection with the aggression of the Russian Federation against Ukraine. It is the responsibility of the state and its authorities to provide adequate and, above all, effective protection for systems and their constituent equipment, facilities, installations as well as services belonging to critical infrastructure.

The first references to the protection of critical infrastructure in Poland (although not directly in such terms), appeared in the Act of 21 November 1967 on the universal duty to defend the People's Republic of Poland[1]. Article 2 of the Act emphasises that all organs of state authority and administration, state institutions, units of the socialised economy, social organisations and every citizen is obliged to strengthen the defence of the People's Republic of Poland and national property in the event of a threat to the security of the State. In addition, Article 2 refers to an extremely important element from the point of view of critical infrastructure, which is cyberspace. Cyberspace should be understood, according to Article 2(1b) of the said Act, as the space for processing and exchanging information created by information and communication systems.[2] The currently in force Act of 11 March 2022 on homeland defence, inter alia, in Article 1, point 19, defines the competence of the authorities in matters of applying for the recognition of an object as particularly important for the security or defence of the state[3]. The essential national legislative acts governing the protection of critical infrastructure are:

[1]Act of 21 November 1967 on the universal duty to defend the People's Republic of Poland, Journal of Laws of 1967 no. 44 item 220.

[2]Act of 17 February 2005 on computerisation of the business entities pursuing public tasks, Journal of Laws of 2005 no. 64 item 565.

[3] Act of 11 March 2022 on homeland defense, Journal of Laws of 2022, item 655; see also Act of 29 August 2002 on martial law and the powers of the Supreme Commander of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland, Journal of Laws of 2002 No. 156 item 1301; Act of 29 August 2002 on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland, Journal of Laws of 2002 No. 156 item 1301.

- Act of 22 August 1997 on the protection of persons and property[4];
- Act of 22 January 1999 on the protection of classified information[5];
- Ordinance of the Council of Ministers of 24 June 2003 on objects of particular importance for state security and defence and their special protection[6];
- Act of 26 April 2007 on crisis management[7];
- and 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.

The first of the aforementioned acts determines, inter alia, the issues concerning the area and transport subject to mandatory protection. Pursuant to Article 5 of the Act, areas, facilities, equipment and transports that are essential for defence, the economic interest of the state, public security and other compelling interests of the state are subject to mandatory protection by specialised armed protection formations or appropriate technical protection. In this respect, a classification of objects, areas, and equipment has been undertaken, namely:

- with regard to national defence (Article 5(2) (1a-c));
- with regard to the protection of the economic interest of the state (Article 5(2) (2a-c));
- with regard to public security (Article 5(2) (3a-c));
- with regard to other compelling interests of the state (Article 5(4) (a-d));
- facilities, including buildings, equipment, installations, services included in the consolidated list of critical infrastructure facilities, installations, equipment and services (Article 5(2) (5)).

In turn, the Act on the protection of classified information of 22 January 1999 covers issues concerning the protection of ICT critical infrastructure. Pursuant to Article 14 of the Act, state protection services (the Internal Security Agency and the Military Counterintelligence Service) are authorised, inter alia, to carry out functions concerning the security of

[4] Journal of Laws of 1997 No. 114 item 74.
[5] Journal of Laws of 1999 Nr 11 item 95.
[6] Journal of Laws of 2003 No. 116 item 1090.
[7] Journal of Laws of 2007 No. 89 item 590.

ICT systems and networks. However, on the basis of Article 1, the Act defines the principles of protection of information that requires protection against unauthorised disclosure, as constituting a state or official secret, regardless of the form and manner of its expression, also in the course of its development, hereinafter referred to as 'classified information'.

The most comprehensive as well as the most important legal act addressing issues concerning the protection of critical infrastructure is the Act on crisis management referred to in point four and the Resolution of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure. The Act on crisis management defines basic concepts such as critical infrastructure, European critical infrastructure, critical infrastructure protection, emergency situation, etc. Pursuant to Article 3(2) of to the Act on crisis management, critical infrastructure is defined as 'systems and their constituent objects, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs'. In turn, Article 3(2) lists individual systems comprising critical infrastructure, which includes the systems of:

a) supply of energy, energy resources and fuels,
b) communications,
c) data communication networks,
d) finance,
e) food supplies,
f) water supply,
g) healthcare,
h) transport,
i) rescue,
j) ensuring continuity of public administration,
k) production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances.

The definition of European critical infrastructure, in turn, can be found in Article 3(2a), of the Act on crisis management, according to which European critical infrastructure consists of systems and their functionally related facilities, including buildings, equipment and installations crucial for the security of the state and its citizens and for ensuring the efficient functioning of public administration bodies, as well as institutions and entrepreneurs, referred to in point 2(a) and (h), with regard to electricity, oil

and gas, road, rail, air, inland waterways transport, ocean and short-sea shipping and ports, located in the territory of the Member States, the disruption or destruction of which would significantly affect two or more Member States. This definition is in conformity with that formulated on the basis of 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[8]. An important aspect in qualifying individual systems as critical infrastructure is the need to meet certain criteria, which are sectoral and cross-cutting in nature[9].

The National Programme for the Protection of Critical Infrastructure was an important document that was first developed and subsequently adopted by the Council of Ministers on 26 March 2013. It has now been revised and updated by 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, taking into account Resolution No. 116/2020 of the Council of Ministers of 13 August 2020 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure and Resolution No. 38 of 21 March 2023 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure. This instrument was developed on the basis of Article 5b of the Act on crisis management, according to which the Council of Ministers adopts, by resolution, the National Programme for the Protection of Critical Infrastructure, hereinafter referred to as 'the programme', the purpose of which is to create conditions for the improvement of the security of critical infrastructure, in particular with regard to: preventing the disruption of critical infrastructure; preparing for emergencies that may adversely affect critical infrastructure; responding to situations of destruction or disruption of critical infrastructure and the restoration of critical infrastructure.

The instrument is divided into twelve parts, which include:

1. basic definitions;
2. scope;
3. objectives;
4. priorities and principles of the programme;

[8] Article 2b of 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, OJ of the European Union 23.12.2008, L 345/75.

[9] Milewski, 2016; Szewczyk and Pyznar, 2010.

5. identification of critical infrastructure;
6. bodies and actors involved in the implementation of the programme;
7. their roles and responsibilities;
8. protection of critical infrastructures;
9. action plan for a period of 2 years following the adoption of the National Critical Infrastructure Protection Programme update by the Council of Ministers;
10. the international aspect of the protection of critical infrastructures;
11. evaluation of the effectiveness of the programme;
12. list of annexes.

The initial part of the document, namely point 1, presents basic definitions related to critical infrastructures including, inter alia, issues such as:

- CI system coordinator,
- CI protection (mandatory, specific),
- CI operator, crisis situation.

Among the main principles guiding the protection programme are: the principle of proportionality and risk-based action, recognition of differences between systems; the leading role of the minister in charge of the system; equality of operators and complementarity[10].

At the end of 2018 and the beginning of 2019, a decision was taken on the need to amend 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. The work led to the development of important legislation at European Union level, namely:

- Regulation of the European Parliament and of the Council (EU) on digital operational resilience for the financial sector;[11]
- Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2);[12]
- Directive on the resilience of critical entities (CER) Directive of 27 December 2022.[13]

[10] It should be noted that there are approximately 760 objects classified as critical infrastructure facilities in Poland, the largest number of which are communication and energy supply facilities, vide: Karolewski, Rejman – Karolewska, 2015, p. 108.

[11] Regulation (EU) of the European Parliament and of the Council of 27 December 2022 on digital operational resilience for the financial sector (OJ EU L 333/1).

[12] Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2) of 27 December 2022. OJ EU L 333/80.

Immediately prior to the promulgation of the aforementioned Directives, the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure[14]. Inter alia, this recommendation identified issues relating to evolving threats such as the war in Ukraine. Point 5 of the recommendations highlights that "in view of the fast-evolving threat landscape, resilience-enhancing measures should be taken as a matter of priority in key sectors such as energy, digital infrastructure, transport and space, and in other relevant sectors identified by the Member States. Such measures should focus on enhancing the resilience of critical infrastructure taking into account relevant risks, especially cascading effects, supply chain disruption, dependence, impacts of climate change, unreliable vendors and partners, and hybrid threats and campaigns including foreign information manipulation and interference." It also stressed that Member States should, in accordance with EU and national law, use all available tools to make progress and contribute to strengthening physical resilience and cyber resilience, as well as strengthening the ability to respond quickly and effectively to disruptions of critical services by critical infrastructure[15].

An important aspect from the point of view of the national critical infrastructure is the proper cooperation and coordination between the authorities responsible for its security. It should be noted that these authorities are extremely numerous, hence there is need to develop appropriate protective procedures. In addition, only proper national legislation, coordinated with European acts, can ensure the proper operation of the relevant state services.

2. Authorities responsible for the protection of critical infrastructure

Given the thematic scope of this study, the main emphasis will be on issues related to the authorities that, within the scope of their powers, have competencies to ensure the protection of critical infrastructures and, in particular, the special services and the Government Security Centre.

---

[13] Directive on the resilience of critical entities (CER) Directive of 27 December 2022. OJ EU L 333/164.

[14] Council Recommendation of 8 December on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (2023/C 20/01).

[15] Ibid paragraphs 7 and 12 of the Council Recommendations.

2.1 Ministers

According to the 2023 National Programme for the Protection of Critical Infrastructure, individual ministers have a specific role in protecting it. The table below shows the list of the ministers responsible for individual critical infrastructure systems.

Table 1 *List of ministers responsible for individual critical infrastructure protection systems.*[16]

Minister responsible for the critical infrastructure system	Critical infrastructure system
1. Minister responsible for state assets. 2. Minister responsible for energy. 3. Minister responsible for the management of mineral deposits.	Energy, energy resources and fuels supply system
1. Minister responsible for information technology. 2. Minister responsible for communications.	Communication system
1. Minister responsible for information technology.	ICT network system
1. Minister responsible for budget. 2. Minister responsible for public finance. 3. Minister responsible for financial institutions.	Financial system
1. Minister responsible for agriculture. 2. Minister responsible for agricultural markets.	Food supply system
1. Minister responsible for water management.	Water supply system
1. Minister responsible for health.	Healthcare system
1. Minister responsible for transport. 2. Minister responsible for maritime	Transport system

[16] National Programme for the Protection of Critical Infrastructure, 2023, p. 18.

affairs.	
1. Minister responsible for home affairs.	Rescue system
1. Minister responsible for information technology.	System for continuity of public administration
1. Minister responsible for climate.	System for production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances

The above list of responsible ministers for individual critical infrastructure protection systems was amended by Resolution of the Council of Ministers No. 116/2020 of 13 August 2020 amending the resolution on the adoption of the National Programme for Critical Infrastructure Protection. As is apparent, one or several ministers may be charged with the responsibility for a particular protection system, depending on the competences assigned. Examples of such systems for which three ministers are responsible are the energy, energy resources and fuels supply system and the financial system.

2.2. Government Centre for Security (RCB)

The Government Centre for Security was established on the basis of Article 10 of the Act of 10 April 2007 on crisis management, which, as a budgetary unit, is subordinate to the Prime Minister. The Government Centre for Security is headed by a director, who is appointed by the Prime Minister.

The RCB's organisational units include:

- Analysis and Response Office, consisting of the Operations and Analysis Department and the Information Policy Department;
- Logistics and Finance Office consisting of Administration and Finance Department, IT and Communications Department, Accounting Department and an Independent Logistics Officer;
- Office of Civil Planning and Critical Infrastructure Protection, which is divided into:

- Department of Risk Assessment and Planning;
- Department of Critical Infrastructure Protection;
- Department of International Cooperation;

- Independent Protection and Control Office and independent position for legislative services.

This body provides services to the Council of Ministers, the Prime Minister, the team and the minister responsible for internal affairs in matters of crisis management and acts as a national crisis management centre. The basic tasks of the Government Centre for Security are described in Article 11(2) of the Act on crisis management. Thus, the tasks of the Government Centre for Security include:

1. civil planning, including:

a) outline specific ways and means of responding to and mitigating risks,
b) developing and updating the National Crisis Management Plan, in cooperation with the relevant organisational units of the offices serving ministers and heads of central offices,
c) analysing and assessing the possibility of risks or their development,
d) gathering information on risks and analysing the material collected,
e) drawing up conclusions and proposals for preventing and countering risks,
f) planning the use of the Armed Forces of the Republic of Poland to perform the tasks referred to in Article 25(3),
g) planning the support by public administration bodies of the implementation of the tasks of the Armed Forces of the Republic of Poland,

2. monitoring potential threats; agreeing crisis management plans drawn up by ministers in charge of government administration departments and heads of central offices,
3. preparing the activation, in the event of emergencies, of crisis management procedures; preparing draft opinions and positions of the team,
4. preparing and providing technical and organisational support for the work of the team,
5. ensuring the coordination of the information policy of public administration bodies during a crisis situation,
6. liaising with entities, cells and organisational units of the North Atlantic Treaty Organisation and the European Union and other

international organisations responsible for crisis management and critical infrastructure protection,

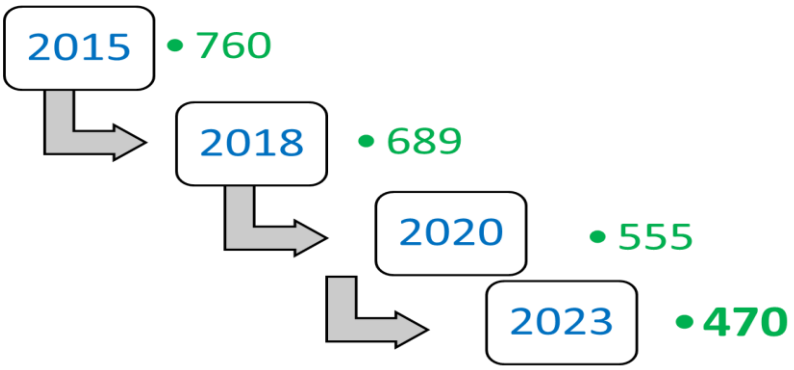
7. organising, conducting and coordinating crisis management training and exercises and participating in national and international exercises,
8. ensuring the circulation of information between national and foreign authorities and crisis management structures; implementation of the tasks of the standby duty within the framework of state defence readiness; implementation of tasks in the field of prevention, counteraction and elimination of the consequences of events of a terrorist nature
9. cooperating with the Head of the Internal Security Agency in preventing, counteracting and removing the effects of terrorist incidents,
10. implementation of planning and program tasks in the field of critical infrastructure protection and European critical infrastructure protection, including the development and updating of the functional annex to the National Crisis Management Plan on critical infrastructure protection, as well as cooperation, as a national point of contact, with the institutions of the European Union and the North Atlantic Treaty Organization and their member countries in the field of critical infrastructure protection,
11. preparation of a draft ordinance of the Prime Minister referred to in Article 7(4) (list of undertakings and procedures of the crisis management system taking into account obligations resulting from membership in the North Atlantic Treaty Organization and bodies responsible for their activation).

The critical infrastructure protection plan should include elements such as: critical infrastructure characteristics (processes implemented, resources); risk assessment (hazard identification, risk analysis, risk assessment), essential options for action (procedures - response), cooperation with state authorities (at local, provincial, national level).

An important element in the scope of the RCB's activities is the need to prepare the National Programme for the Protection of Critical Infrastructure. In addition, the RCB performs the function of a national Crisis Management Centre.

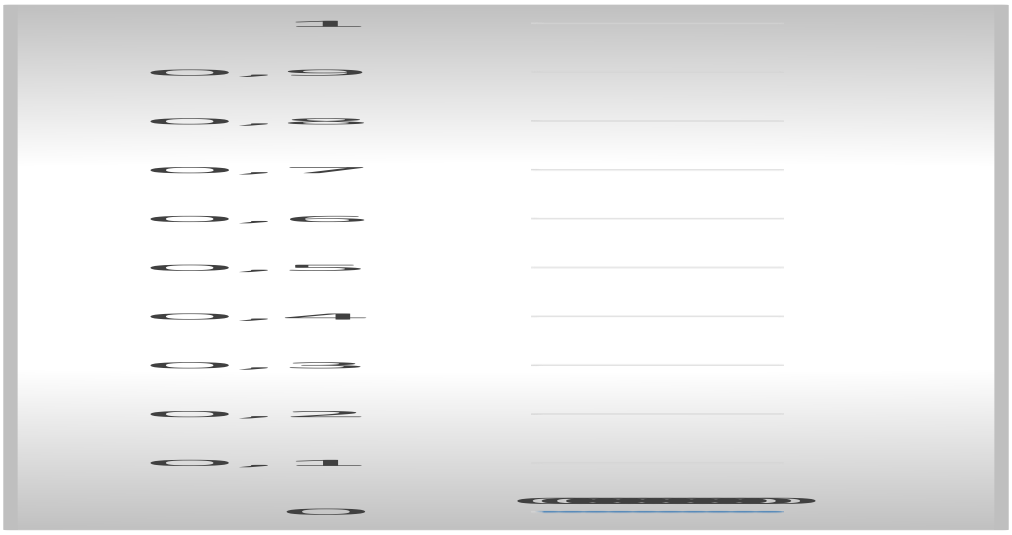
The chart below presents a list of critical infrastructure facilities in Poland.

Figure 1 *Number of critical infrastructure facilities between 2015 and 2023.*[17]



In turn, the chart below shows the quantitative distribution of critical infrastructure facilities in critical infrastructure systems in 2020.

Figure 2 *Quantitative distribution of critical infrastructure facilities in critical infrastructure systems in 2020.*[18]



[17] GCS (Polish: RCB – Rządowe Centrum Bezpieczeństwa, [Online]. Available at: https://www.gov.pl/web/rcb (Accessed: 17 December 2024).
[18] RCB, [Online]. Available at: https://www.gov.pl/web/rcb (Accessed: 17 December 2024).

- 252-energy supply infrastructure
- 124-telecommunication infrastructure
- 61-water supply infrastructure
- 57-transport infrastructure
- 23-infrastructure ensuring continuity
- 18-rescue infrastructure
- 17-financial infrastructure
- 8-ICT networks infrastructure
- 3-medical infrastructure
- 2-production and storage facilities.

As is apparent, the largest number of critical infrastructure facilities are energy supply and communications facilities (376 facilities out of 555). One of the most important organisational units of the RCB is the Operations and Analysis Department, which is part of the Analysis and Response Office. Its main tasks include: coordinating the circulation of information, monitoring and risk analysis, preparing and activating crisis management procedures. As was correctly ascertained in the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, it contributes to broader efforts to counter hybrid threats and campaigns against the Union and its Member States. The need to ensure the protection of facilities and equipment belonging to critical infrastructure is a key guarantor of national security. The recent EU directives mentioned above indicate the importance of ensuring the protection of critical infrastructures, which directly translates into security in a global sense.

2.3. The Internal Security Agency (ABW)

One of the special services that plays a fundamental role in the security of the state, its constitutional order, including, inter alia, the protection of critical infrastructure, is the Internal Security Agency (ABW). It is a special service which was created on 29 June 2002[19] after the dissolution of the Office of State Protection. As a result of the dissolution of the Office of State Protection, two civilian special services were separated, the Internal Security Agency and the Foreign Intelligence Agency.

[19] Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, Journal of Laws of 2023, item 1136.

The tasks of the Internal Security Agency are set out in Article 5 of the Act, according to which the ABW is, inter alia, responsible for:
1) identifying, preventing and combatting threats to the internal security of the State and its constitutional order, and in particular to the sovereignty and international standing, independence and inviolability of its territory, as well as to the defence of the State;
2) the identification, prevention and detection of the following crimes:
(a) espionage, terrorism, unlawful disclosure or use of classified information and other offences against state security,
(b) crimes that harm the economic basis of the state,
(c) corruption of persons performing public functions, as referred to in Articles 1 and 2 of the Act of 21 August 1997 on restrictions on the conduct of business activities by persons performing public functions (Journal of Laws of 2022, item 1110, and of 2023, item 497), if this may harm state security,
(d) production and marketing of goods, technologies and services of strategic importance for state security,
(e) the illicit manufacture, possession and trafficking of arms, munitions and explosives, weapons of mass destruction and narcotic drugs and psychotropic substances, in international traffic,
(f) act against the administration of justice, referred to in Article 232, Article 233, Article 234, Article 235, Article 236 § 1 and Article 239 § 1 of the Act of 6 June 1997. - Criminal Code (Journal of Laws of 2022, item 1138, 1726, 1855, 2339 and 2600 and of 2023, item 289), if they remain in connection with the offences referred to in items (a)-(e) and prosecution of their perpetrators;
2a) identification, prevention and detection of threats to the security, relevant to the continuity of the state's functioning, of ICT systems of public administration bodies or ICT network system covered by the uniform list of objects, installations, devices and services constituting critical infrastructure, as well as ICT systems of owners and holders of objects, installations or devices of critical infrastructure, referred to in Article 5b (7) item 1 of the Act of 26 April 2007 on crisis management (Journal of Laws of 2023, item 122)[20];
2b) the disclosure of property threatened with forfeiture in connection with the offences referred to in point 2;

[20] Ibid.

3) carrying out, within the limits of its competence, tasks relating to the protection of classified information and performing the functions of a national security authority with regard to the protection of classified information in international relations;
4) obtaining, analysing, processing and transmitting to the competent authorities information likely to be of importance for the protection of the State's internal security and constitutional order;
5) undertaking other activities specified in separate acts and international agreements[21].

Additionally, the activity of the Internal Security Agency outside the borders of the Republic of Poland may be carried out in connection with its activity on the territory of the State only within the scope of the performance of the tasks set out in section 1 item 2(3). The Head of the Internal Security Agency shall perform the tasks of the contact point for data exchange referred to in Article 16(3) of the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12)[22].

With regard to the tasks of the Internal Security Agency, it is important to emphasise that the Constitutional Tribunal, in its ruling of 30 July 2014, expressed its opinion on Article 5(1)(2)(a) of the Act on Internal Security Agency and Foreign Intelligence Agency insofar as it includes the phrase "and other offences detrimental to state security", as well as on Article 5(1)(2)(c) of Act on Internal Security Agency and Foreign Intelligence Agency. This is attributable to the fact that the wording raised doubts as to the scope of the service's activities. In its judgment, it ruled, inter alia, that: "The values protected in Article 5 of the Internal Security Agency and Foreign Intelligence Agency Act are covered by the content of the following notions: state security, internal security of the state and its constitutional order, sovereignty and international position of the state, inviolability of its territory, defence of the state, economic basis of the state, as well as, inter alia, public morality and efficiency of functioning of state institutions, international legal obligations of the state with their axiological premises. By their very nature, these constitutionally significant values

[21] Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, Journal of Laws of 2023, item 1136.
[22] Article 16(3) of the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

cannot be specified in detail in the law, hence the necessity for the legislator to use a general concept, 'collecting' specific values"[23].

2.4. ICT security

It is worth noting that one of the key tasks of the Internal Security Agency is to ensure the state's ICT security. According to the Act of 21 December 2001 amending the Act on the organisation and operational mode of the Council of Ministers and the scope of ministers' activities, the Act on divisions of government administration as well as amending some acts[24], the modern information and communication technologies include the need to ensure security of: IT infrastructure, ICT systems as well as networks and information technology, technology and IT standards.

Besides, it is necessary to support investments in the field of information technology, information education as well as ICT and multimedia services. At the same time, Poland is obliged to apply information technology in the information society, in particular in the economy, banking and education, and to fulfil the international obligations of the Republic of Poland in the field of information technology[25]. In addition, in the Act of 5 August 2010 on the protection of classified information[26] in Chapter 8, on may discover in Articles 48-53, provisions on ICT security of systems and networks in which classified information is processed. Furthermore, in the Regulation of the Prime Minister of 20 July 2011 on basic requirements of information and communication security[27], one can find issues concerning the so-called electromagnetic protection of an information and communication system, which is intended to prevent and counteract a breach of confidentiality and availability of classified information processed in an information and communication system. An important aspect related to ICT security, is the possibility of a potential terrorist threat, which can trigger so-called network incidents. In this regard, the relatively newly enacted Act of 5 July 2018 on the national cyber security system[28], which implements Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning

[23] Judgment of the Constitutional Tribunal of 30 July 2014, ref. K 23/11.
[24] OJ. 2001, item 1800.
[25] Poterała, 2021.
[26] Journal of Laws of 2005, item 1631 as amended.
[27] OJ. 2011, item 948.
[28] OJ. 2020, item 1369.

measures for a high common level of security of network and information systems across the Union [29], plays a key role. Article 1 of the Act defines the organisation of the national cyber security system and the tasks and responsibilities of the entities comprising this system; the manner of supervision and control in the application of the provisions of the Act as well as the scope of the Cyber Security Strategy of the Republic of Poland. In addition, there are also defined basic concepts such as: cyber security, defined as the immunity of information systems to activities that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems, as well as incidents defined as an event that has or may have an adverse impact on cyber security, including their division into incidents: critical, serious and significant incidents[30]. The ICT security system has been based on the so-called CSIRTs (Computer Security Incident Response Team). Within the scope of competence of the Head of the ABW remain ICT systems and ICT networks, covered by the uniform list of objects, installations, devices and services included in the critical infrastructure, referred to in Article 5b(7)(1) of the Act on crisis management. In addition, the ABW carries out its statutory tasks concerning terrorist incidents in cyberspace, as well as tasks of a preventive nature[31].

2.5. Espionage and terrorism

On the basis of Article 5(1) (2a), the tasks of the Internal Security Agency also include the identification, prevention and detection of offences such as espionage and terrorism. The criminal threats for the crime of espionage are in turn described in Article 130 of the Criminal Code, according to which: "Whoever takes part in the activities of a foreign intelligence service or acts on its behalf, against the Republic of Poland, shall be subject to the penalty of deprivation of liberty for a term not shorter than 5 years (§ 1); Whoever, taking part in the activities of a foreign intelligence service or acting on its behalf, provides this intelligence service with information the transmission of which may cause damage to the Republic of Poland, shall be subject to the penalty of deprivation of liberty for a term not shorter than 8 years or life imprisonment (§ 2); Whoever declares readiness to act for the benefit of foreign intelligence against the Republic of Poland or in order to provide foreign intelligence with information the transmission of which may cause

[29] OJ EU L 194, 19.07.2016, p. 1.
[30] Article 2 of the Act of 5 July 2018 on the National Cyber Security System.
[31] Poterała, 2021, pp. 89-117.

damage to the Republic of Poland, collects or stores such information or enters an information system in order to obtain it, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years (§ 3)".

In addition, subsequent articles provide for penalties for organising or directing the activities of a foreign intelligence service, for taking part in the activities of a foreign intelligence service not directed against the Republic of Poland and conducted on its territory without the consent of the competent authority granted under separate provisions, as well as for preparation for the aforementioned offences. In recent years, in connection with the intensification of intelligence activities mainly on the part of Russia, the legislator decided to increase the criminal threat for the offence of espionage. The offence of espionage has also been amended to comprise taking part in the activities of a foreign intelligence service or acting on its behalf, conducting disinformation by disseminating false or misleading information with the aim of causing serious disturbance to the system or economy of the Republic of Poland, an allied country or an international organisation of which the Republic of Poland is a member, or inducing a public authority of the Republic of Poland, an allied country or an international organisation of which the Republic of Poland is a member to take or refrain from taking certain actions.

Activities directly related to espionage are also acts of terrorism. Certainly, the enactment of the Act on anti-terrorist activities[32] on 10 June 2016 was a great support for counter-terrorist activities. In this law, in addition to defining basic definitions such as anti-terrorist and counter-terrorist activities, there are also definitions concerning public administration infrastructure or indications concerning critical infrastructure which refer directly to the aforementioned Act of 26 April 2007 on crisis management. According to Article 3 paragraph 1, the Head of the Internal Security Agency, hereinafter referred to as the 'Head of the Internal Security Agency', is responsible for the prevention of terrorist incidents, in turn, the minister in charge of internal affairs is responsible for preparing to take control of terrorist incidents through planned undertakings, responding in the event of the occurrence of such incidents and restoring resources to respond to such incidents. The present Act has been divided into seven chapters, of which the provisions relating to actions to prevent terrorist incidents (Chapter 2), alert degrees (Chapter 3) as well as anti-terrorist

[32] OJ 2021, item 2234 as amended.

actions at the scene of a terrorist incident, including counter-terrorist actions (Chapter 4) are of particular importance. Particularly important powers have been conferred on the Head of the Internal Security Agency in Article 9 of the cited Act. Pursuant to this provision, in order to recognise, prevent, combat and detect offences of a terrorist nature or an offence of espionage and to prosecute their perpetrators, the Head of the Internal Security Agency may order, for a period of no longer than 3 months, the discreet conduct of activities with regard to a person who is not a citizen of the Republic of Poland, with regard to whom there is a concern as to the possibility of his/her conducting terrorist activity or committing an offence of espionage, consisting of: obtaining and recording the content of conversations conducted by technical means, including by means of telecommunications networks, obtaining and recording images or sound of persons from premises, means of transport or places other than public places, obtaining and recording the content of correspondence, including correspondence conducted by means of electronic communication, obtaining and recording data contained on computer data carriers, telecommunications terminal equipment, information and data communication systems, gaining access to and controlling the contents of consignments.

An important role in combatting terrorist threats is played by the Anti-Terrorist Centre (CAT), established on the basis of: the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, the Act of 10 June 2016 on anti-terrorist activities and Order No. 163 of the Prime Minister of 26 September 2018 on granting the statute of the Internal Security Agency.

The Anti-Terrorist Centre's role is to coordinate the process of information sharing between participants in the counter-terrorism defence system and to implement timely joint response procedures in the event of the occurrence of one of the four categories of defined threat: a terrorist event on Polish territory affecting the security of Poland and its citizens, a terrorist event occurring outside the borders of the Republic of Poland, affecting the security of the Republic of Poland and its citizens, obtain information on potential threats that may occur in Poland and abroad and obtaining information on 'money laundering' or financial transfers that may be indicative of the financing of terrorist activities[33].

The Centre operates on a 24/7 basis. The service in the unit is performed by officers, soldiers and civilian employees of national entities

[33] Obuchowicz, 2010, pp. 275 et seq.

dealing with counteracting terrorist threats, i.e. the Foreign Intelligence Agency, the Internal Security Agency, the Military Intelligence Service, the Military Counterintelligence Service. The service in this unit may also be performed by officers of: Polish National Police, Polish Border Guard, State Protection Service, State Fire Service, National Fiscal Administration, Military Police and the Government Security Centre[34]. In addition to the Anti-Terrorist Centre, there is also the Terrorist Prevention Centre at the Internal Security Agency, which, being a specialised unit, deals with broadly understood anti-terrorist prevention[35].

It should also be added that on the basis of the Order of the National Public Prosecutor in the Mazovian Branch of the Department for Organised Crime and Corruption of the National Public Prosecutor's Office in Warsaw, the Espionage Unit was established on 24 September 2018. Prosecutors performing their duties in this division supervise proceedings conducted by the Internal Security Agency concerning crimes of espionage, disinformation and terrorist acts. In conclusion, it is worth noting that the most recent surveys on both terrorism in Poland and the directions of its development clearly indicate that

> in the opinion of a large percentage of respondents, Poland may become an attractive country for terrorists. Although there has been little indication of this in recent years, the belief that the situation will deteriorate in the near future seems to be quite widespread. (...) Concerns are at least partly related to threats coming from Russia[36].

It is worth quoting the partial results of a survey conducted in April 2022 by Internal Security Agency officers among academics and representatives of services and institutions belonging to the anti-terrorism community involved in terrorism studies. The results of the survey clearly indicate that, according to the respondents, critical infrastructure facilities are the most 'popular' in the sphere of a terrorist attack within the European Union at 39.3%, followed by open urban spaces (32.9%), then by tourist infrastructure and sports facilities (14.8%), military bases (7.4%) and

[34] Kolaszyński, 1989, p.14.
[35] Available at: https://Centrum Prewencji Terrorystycznej ABW (tpcoe.gov.pl)), (Accessed: 22 January 2024).
[36] Vidino, 2023, p. 254.

government office buildings (5.3%). On the other hand, in terms of the answer to the question: which tools, devices or technologies present the most significant security risks to citizens from the perspective of services, the largest group of respondents, 69.1%, answered that it is the unmanned aerial vehicles. When asked which terrorist organisation posed the greatest threat to the security of EU countries, the vast majority answered that it was ISIS (62.7%), followed by Al-Qaida (15.9%) and the Russian Federation's special services (11.7%). It is also worth noting the question related to the greatest technological challenge for ICT security services. According to respondents, these are: highly advanced control process automation technologies (35.1%), artificial intelligence (26.6%) and cloud storage (22.3%). This was followed by the development of 5G transmission standards (12.7%), quantum technology (2.1%) and encryption of communications (1%)[37].

3. Summary

The protection of critical infrastructures today is particularly important from the point of view of the society and has a transnational as well as a multidimensional dimension. Only a correct assessment of threats, their estimation and counteraction can lead to a reduction of the negative effects associated with the danger of their occurrence. Also of importance are the National Programmes for the Protection of Critical Infrastructure, which are prepared and adapted to current situations; the Government Centre for Security, which cooperates with ministers and heads of central offices competent in matters of national security, is responsible for drafting them. It is evident that only through mutual international cooperation and collaboration in the field of critical infrastructure protection can we effectively mitigate risks, enhance early detection capabilities, and prevent crises. To this end, it is necessary to ensure a common European security policy and, consequently, to develop legal solutions of an international and supra-regional nature. The dynamics of the change in today's security environment requires a systematic response and the introduction of new legal solutions. Examples of such solutions are, for example, those mentioned in this publication:

[37] Szlachter, 2022, pp. 148-185.

- Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2) of 14 December 2022[38],
- 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
- Directive on the resilience of critical entities (CER) of 14 December 2022, repealing Council Directive 2008/114/EC[39].

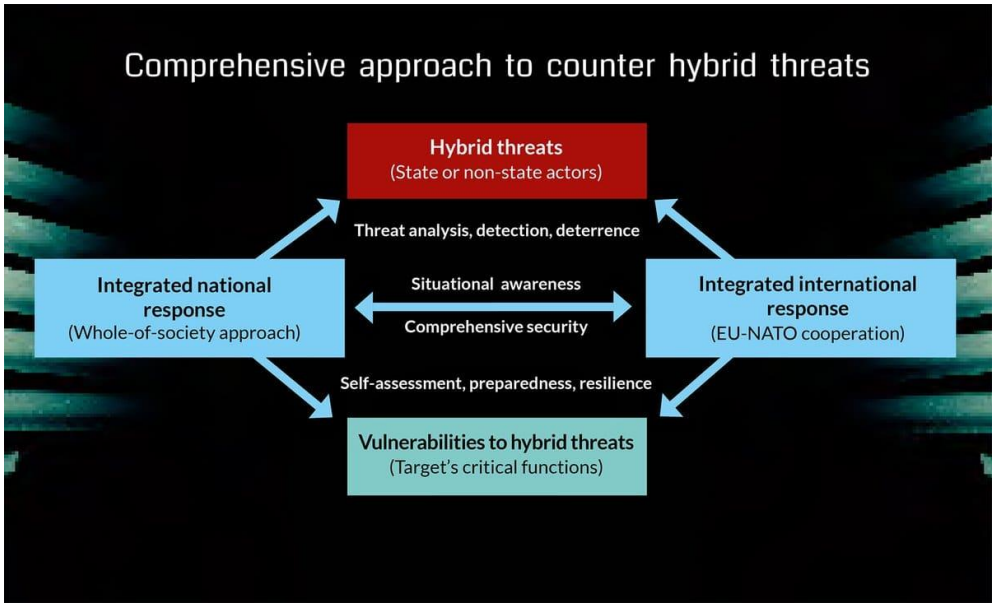
Moreover, a key document of exceptional importance for the security of EU countries is the developed EU Security Strategy, which contains common assumptions for ensuring security.

An important aspect concerning the need to undertake urgent changes at least in the legislative field is the issue of the so-called hybrid threats. In 2016, the European Commission and the European External Action Service (EEAS) developed a Joint Framework on countering hybrid threats a European Union response, containing 22 actions to be taken by Union Member States and institutions to identify hybrid threats, raise awareness of these threats, and take steps to build resilience[40].

In April 2017, an agreement was signed in Helsinki about a centre to combat hybrid threats, of which Poland and 18 other countries are members. The main threats listed include propaganda threats, cyber threats and disinformation in the broadest sense. The chart below shows a comprehensive approach to hybrid threats.

[38] Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2) of 27 December 2022. OJ EU L 333/80.
[39] Directive on the resilience of critical entities (CER) Directive of 27 December 2022. OJ EU L 333/164.
[40] Available at: https://www.nato.int/docu/review/pl/articles/2018/11/23/ (Accessed: 23 January 2024).

Figure 3 *Comprehensive approach to hybrid threats*[41]



The demands made years ago on the need to develop IT-based threat knowledge management as well as the development of a risk assessment model to properly respond to possible threats seem right. Such a model can certainly contribute to the broader optics of managing the issues of possible threats[42].

[41] NATO, [Online]. Available at: https://www.nato.int (Accessed: 23 January 2024).
[42] Trocicka, 2019.

Bibliography

[1] Milewski, J. (2016) ‘Identyfikacja infrastruktury krytycznej i jej zagrożeń. Systemowe wymogi bezpieczeństwa’ [Identification of critical infrastructure and its threats. Systemic security requirements], *Zeszyty Naukowe AON*, 4(105), pp. 99-115.

[2] Szewczyk, T., Pyznar, M. (2010) ‘Ochrona infrastruktury krytycznej a zagrożenia asymetryczne’ [Critical infrastructure protection against asymmetric threats], *Przegląd Bezpieczeństwa Wewnętrznego*, 2(2), pp. 55-56.

[3] Karolewski, A., Rejman – Karolewska, M. (2015) ‘Ochrona infrastruktury krytycznej, Przegląd naukowo – metodyczny’ [Protection of critical infrastructure, Scientific and methodical review]. *Edukacja dla bezpieczeństwa*, 2/2015 (27), p. 108.

[4] Poterała, G. (2021) ‘Zadania ABW w zakresie bezpieczeństwa teleinformatycznego państwa’ [Tasks of the ABW in the field of information and communication security of the state] in: Burczaniuk, P. (ed.) *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego* [Legal aspects of the functioning of special services on the example of the Internal Security Agency]. Warszawa: DIG Publishing House, pp. 89-117.

[5] Obuchowicz, M. (2010) ‘Pięć lat funkcjonowania Centrum Antyterrorystycznego ABW (2008-2013)’ [Five years of functioning of the ABW Antiterrorist Centre (2008-2013)], *Przegląd Bezpieczeństwa Wewnętrznego*, 10, pp. 275 et seq.

[6] Kolaszyński, M. (2016) *Status ustrojowy polskich służb specjalnych po 1989 roku*. [Regime status of Polish secret services after 1989], Kraków: Jagiellonian University Publishing House.

[7] Vidino, L. (2023) ‘Badania ankietowe poświęcone terroryzmowi w Polsce i kierunkom jego rozwoju’ [Survey research on terrorism in Poland and directions of its development], *Terroryzm, studia, analizy, prewencja* [Terrorism, studies, analysis, prevention], 2023(4), p. 254.

[8] Szlachter, D. (2022) ‘Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych’ [Terrorism in Poland and directions of its development. Survey results (abridged report)], *Terroryzm, studia, analizy, prewencja* [Terrorism, studies, analysis, prevention], 2022(2), pp. 148-185.

[9] Trocicka, J. W. (2019) ‘Metodyka typowania i szacowania ryzyka zagrożeń dla bezpieczeństwa państwa’ [Methodology of typing and estimating the risk of threats to state security] in Kośmider, T., Kołtun, L. (eds.) *Współczesny wymiar bezpieczeństwa publicznego. Kształtowanie bezpiecznych przestrzeni. Działania profilaktyczne*. [Contemporary dimension of public security. Shaping safe spaces. Preventive actions], Warszawa: IWS Publishing House.