Iceland
Liechtenstein
Norway grants

frse
Fundacja Rozwoju Systemu Edukacji

TEACHING SCRIPT

SUBJECT:

Management of technical infrastructure protection

author:

dr Adam Włodarczyk, prof. WSPA

Script was developed as a part of the project «Management in time of crisis»

The project „Management in time of crisis" benefits from a € 65,518.00 grant from Iceland, Liechtenstein and Norway under the EEA Grants. The aim of the project „Management in time of crisis" is to adjust the educational e-offer and the method of managing the didactic process at the university to the changing realities of teaching related to the need to function in a situation of a permanent crisis.

Wyższa Szkoła
Przedsiębiorczości
i Administracji

HÁSKÓLINN Á BIFRÖST
BIFRÖST UNIVERSITY

Contents

Introduction

The progress of civilization that we have witnessed in recent years is dynamizing the development of key areas such as education, health care, transportation and energy. Technological progress, which is the driving force of development in many areas that improve the living standards of citizens, at the same time brings with it many new risks. One of the important priorities of any state is to ensure the security of its citizens. If, in any important area, disruptions occur, we observe a decrease in the perceived comfort of life of citizens and a decrease in the sense of security. In view of the above, it becomes a key task to ensure the protection of critical infrastructure, defined briefly as objects and areas of particular importance for the security and defense of the state.

Critical infrastructure (CI) is the foundation of a smoothly functioning state, security and citizens' comfort level. Nowadays, ensuring the resilience of CI is becoming more important than it was years ago. With the development of civilization, CI protection systems are increasingly complex and interactively interconnected, so they are increasingly vulnerable to a variety of threats to their proper functioning. A key factor determining the level of threats is the current geopolitical situation and the emergence of new sources of threats, including those arising from, among other things, so-called "hybrid" activities, which increasingly target critical infrastructure.

The purpose of the study is to present selected issues in the field of issues related to the state's critical infrastructure, its characteristics and methods of protection and the role of government, local authorities and organizations in efforts to ensure the protection of critical infrastructure.

Critical infrastructure protection is a complex task that requires cooperation between the public and private sectors and constant monitoring and adaptation to changing threats. The added value flowing from technological advances is the growing importance of information technology and cyber security in CI protection due to the presence of a huge number of information systems in various critical infrastructure sectors.

Particularly in the current situation, Poland but also other EU countries need "resilient" and highly efficient coordination of CI protection implemented with all available methods and tools. In this regard, the readiness of administrations, services and operators to respond to incidents resulting from escalation of natural, technical, terrorist, or hybrid threats (facsimiles, cyber attacks) becomes crucial. A huge role in enhancing the aforementioned resilience is played by education in those areas that are specific to CI threats, equipping those involved in CI systems with the appropriate resources and competencies. In the current geopolitical situation, CI operators in particular need information, standards for dealing with emergencies and organizational support and knowledge of new solutions for building CI resilience, and the public needs education for security. Security is a state that provides a sense of certainty and guarantees of its preservation and opportunities for improvement. It is one of the basic human needs. It is marked by the absence of the risk of losing something particularly valuable to a person - life, health, work, respect, feelings, tangible and intangible[1]. Security is also a need of states and international systems. Its absence causes anxiety and a sense of threat. A person, a social group, a state, an international organization try to influence their external environment and internal sphere to remove, or at least ward off, threats, eliminating their own fear, anxieties, anxiety and uncertainty.[2] A key role in creating and maintaining national security is played by the state, as the highest form of organization of society's life. The main purpose and essence of security is to secure national interests, headed by ensuring survival, successful existence and conditions for development. Nowadays, a sense of security is associated not only with the absence of external threats, but mainly with ensuring the efficiency of the functioning of the state's broadly understood infrastructure, both in its technical part (manufacturing enterprises, energy, communications, ICT systems, transportation or communications) and social part (health care, rescue and civil protection,

[1] W. Łepkowski, Słownik terminów z zakresu bezpieczeństwa narodowego, AON, Warszawa, 2002 [w:] B. Grenda, J. Nowak, Wybrane problemy zarządzania kryzysowego w organizacjach lotniczych, Akademia Obrony Narodowej, Warszawa 2013, s. 9.

[2] Ibid. s. 9

education, etc.). This part of the infrastructure used to be defined by the term "critical infrastructure"[3] .

The complexity of this system and its sensitivity makes it vulnerable to a wide range of external and internal threats. These incidents can be caused either by forces of nature or as a consequence of human action, as a result of which critical infrastructure can be destroyed, damaged, disrupted and thus cause a threat to the life and property of the public. In view of the possible threats to critical infrastructure, an important issue is to ensure its protection, understood as all activities aimed at ensuring the functionality, continuity of operations and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities, and to reduce and neutralize their effects, as well as the rapid restoration of this infrastructure in the event of failures, attacks and other events that disrupt its proper functioning . As in other countries, also in Poland, a modern and efficient critical infrastructure, regardless of emerging threats, is a decisive factor in the effectiveness of state functioning. In emergency situations, it also determines de facto its survival.

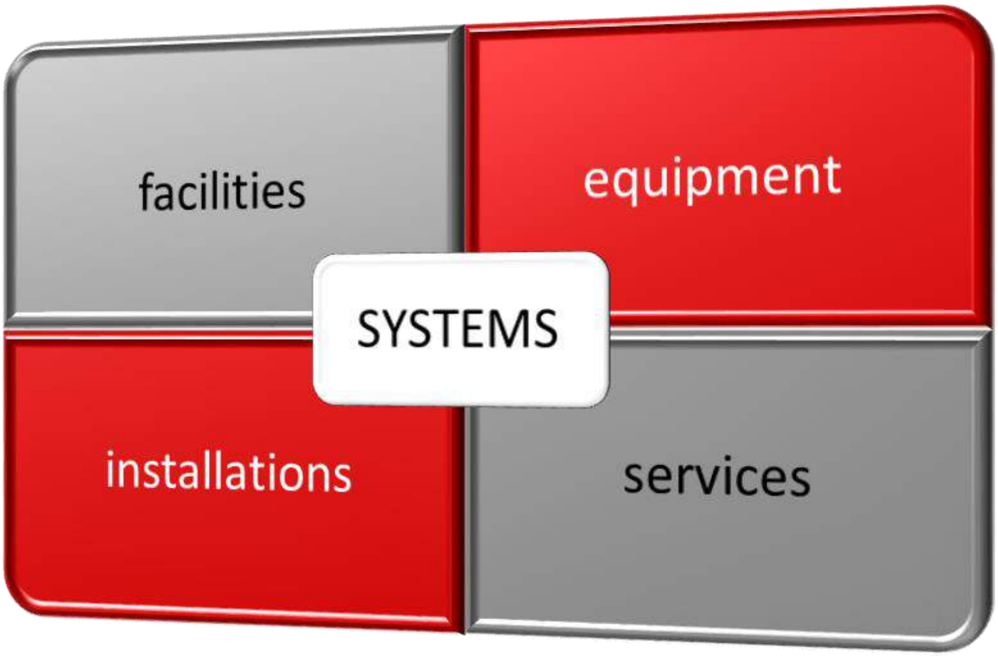
Private companies are the operators of much of the infrastructure critical to state security. Hence, cooperation with business is one of the essential elements to ensure efficient and comprehensive protection of critical infrastructure. It remains important, therefore, to develop transparent rules and procedures for cooperation between the administration and the owners of facilities, installations and/or equipment of critical infrastructure, particularly with regard to the exchange of information, channels for the flow of information from state services, or ensuring the security of data, which are trade secrets of operators.

[3] W. Lidwa, W. Krzeszowski, W. Więcek ,P. Kamiński, Ochrona infrastruktury krytycznej, Akademia Obrony Narodowej, Warszawa 2012, s.7.

1. Critical infrastructure systems – conceptual analysis and legal basis for critical infrastructure protection

Critical infrastructure (CI) is defined as systems and their constituent functionally related 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.[4]

Figure 1. Critical infrastructure



Source: National Critical Infrastructure Protection Program – consolidated text, 2023.

Critical infrastructure systems (CIS) are key elements that ensure the functioning of society, the economy and the state. Protecting these systems is a priority, as their damage or disruption can have serious consequences for national security, social and economic stability, and public health.

[4] Act of April 26, 2007 on crisis management (Journal of Laws 2013, item 1166 and 2015 item 1485).

In the Republic of Poland, critical infrastructure includes 11 systems (facilities, equipment) that are crucial to the security of the state and its citizens and serve to ensure the smooth functioning of public administration bodies, as well as institutions and businesses. These include:[5]

1. Energy, energy resources and fuel supply systems: for the production, transmission and distribution of electricity (power generation), for the production, transportation and distribution of gaseous fuels, for the production, transportation and distribution of oil and petroleum products, for the production, transportation and distribution of heat.
2. Communication systems, ensuring the transmission of information, including mail and telecommunications, as well as radio and television.
3. Data communications networks, a set of cooperating information technology equipment and software, providing for the processing and storage, as well as the sending and receiving of data over telecommunications networks by means of an appropriate, for a given type of network, terminal device.
4. Financial systems, i.e. a set of legal norms and a set of financial institutions whose task is to collect, distribute and disburse the state's monetary resources.
5. Food supply system - the field of economy, which consists of the production of production inputs (e.g., fertilizers, fodder) and services for agriculture, production and procurement of food raw materials (in agriculture, fishing, forestry, hunting), purchase of food raw materials, their storage and transportation, processing of food raw materials, commodity trade in food products (food storage and warehousing, wholesale and retail trade, export and import), and the food safety system covering all components of the food supply chain.
6. Water supply system (drinking water, wastewater, surface water) - it includeș interconnected enterprises and facilities for collecting, refining, supplying and treating water for the population and industry.

[5] Sadowski J., Ochrona infrastruktury krytycznej. Uregulo- wania prawne, Autobusy: technika, eksploatacja, systemy transportowe, 2018, nr 6; Romana Ł, Cygańczuk K., Prawny wymiar ochrony infrastruktury krytycznej – wybrane aspekty, Safety&Fire Technology, Vol. 59, Issue 1, 2022.

7. Health care system (pharmacies, hospitals, clinics) - a set of people and institutions tasked with providing health care to the population. Its efficient functioning (along with the emergency system) is a guarantor of the citizen's rights enshrined in the Constitution.
8. Transportation systems (roads, railroads, airports, ports) - that is, the ability to move people, cargo (the object of transport) in space using appropriate means of transport.
9. Rescue systems - the totality of organizational measures and undertakings undertaken to save health and life, property and the environment, being in danger, and to predict, recognize and eliminate the consequences of events.
10. Systems to ensure the continuity of public administration, that is, the exercise of the right of sovereign performance of tasks assigned by the legal order to the state and its bodies or other entities performing sovereign functions.
11. Systems for the production of storage, storage and use of chemical and radioactive substances (including pipelines of hazardous substances).

The list of critical infrastructure is a so-called unified list of facilities, installations, equipment and services included in critical infrastructure by system. Based on the criteria under article 3(2) of the Law on Crisis Management (UZK), it is compiled by the Director of the Government Security Center (RCB) in cooperation with the relevant ministers responsible for individual systems and competent in matters of national security. The list also distinguishes European critical infrastructure, located on the territory of Poland, and European critical infrastructure, located on the territory of other EU member states, which may have a significant impact on the Polish state. The list of critical infrastructures is not generally available, it is classified in nature (Article 5b Section 7(1) of the UZK).

Extracts are made from the uniform list of facilities, installations, equipment and services included in the critical infrastructure, which are provided to the relevant ministers, heads of central offices responsible for the system in question, voivodes, as well as owners, possessors and dependent owners of facilities, installations or equipment included in the critical infrastructure. The legislation assumes that the obligations of owners and holders of critical infrastructure derive from the law, so the mere notification of inclusion in the list does not have the character of a law. It is a purely informational activity that is not subject to appeal by the owner or holder of critical infrastructure.

Critical infrastructure must be identified, the criteria for its identification are given in Article 3(2) of the UZK, but they are quite general, so the so-called "detailed criteria" contained in the National Critical Infrastructure Protection Program (NPOIK), which is being developed by the Council of Ministers (Article 5b(2)(3) of the UZK) may be helpful. They provide an auxiliary tool for identifying critical infrastructure elements for the RCB Director, acting in cooperation with the relevant ministers. The delineation is carried out without the participation of the owners or holders of critical infrastructure, although, if their critical infrastructure is included in the list, it means that they must comply with their obligations under the Act. This is because the obligation to protect critical infrastructure rests with the legal and de facto owners of critical infrastructure, who are subject to a number of obligations arising not only from the UZK, but also from other laws.

The detailed criteria for distinguishing the facilities, installations, equipment and services that are part of critical infrastructure systems, which serve to assist the RCB Director, can be found in the annex to the 2020 NPOIK, but it is not public.[6]

Critical infrastructure plays a key role in the functioning of the state and the lives of its citizens. As a result of events caused by natural forces or as a consequence of human actions, critical infrastructure can be destroyed, damaged, and its operation can be disrupted, so that the lives and property of citizens can be endangered. At the same time, such events negatively affect the economic development of the country. Hence, **the protection of critical infrastructure is one of the priorities facing the Polish state**. The essence of the tasks related to critical infrastructure boils down not only to ensuring its protection from threats, but also to ensuring that any damage and disruptions to its functioning are as short-lived as

[6] Długosz T., Infrastruktura krytyczna – ochrona infrastruktury krytycznej, https://www.energetyka.plus/infrastruktura-krytyczna-ochrona-infrastruktury-krytycznej/

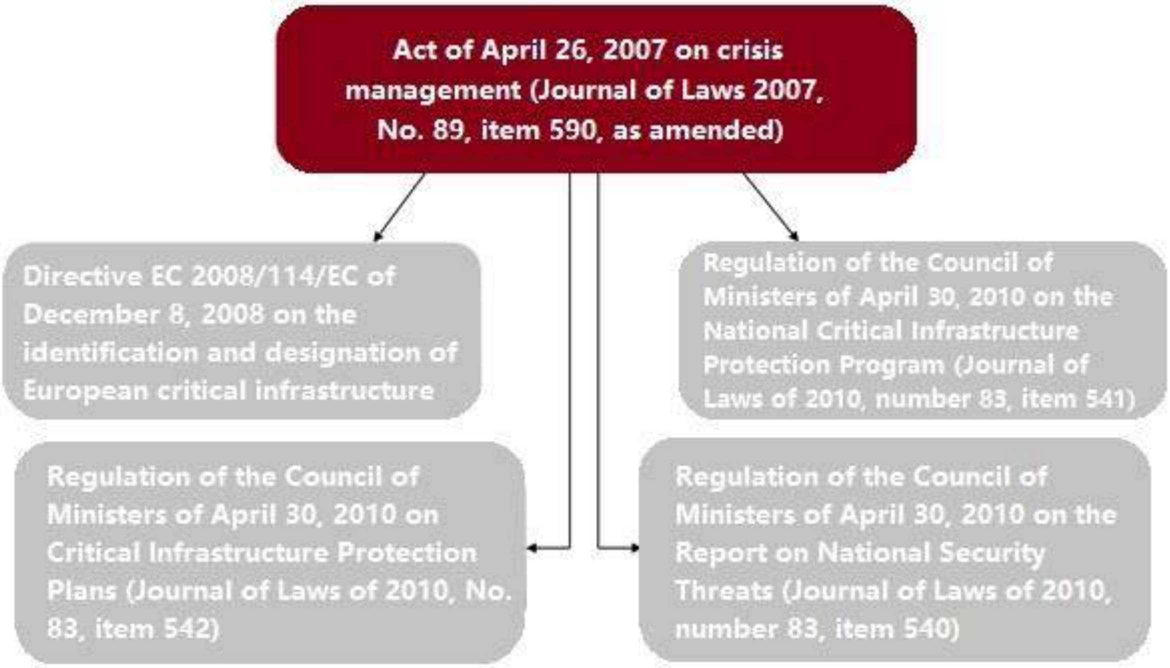
possible, easy to remove and do not cause additional losses to citizens and the economy.

The protection of critical infrastructure stems from Article 6 (5) of the Law on Emergency Management, according to which the owners and possessors, whether sole or dependent, of facilities, installations or equipment identified as critical infrastructure have a duty to protect them. In particular, by preparing and implementing, in accordance with anticipated threats, plans for the protection of critical infrastructure and maintaining their own backup systems to ensure security and sustain its operation until it is fully restored. From this follows the general obligation to secure facilities, installations or equipment identified as critical infrastructure, regardless of the legal title to them, and therefore by all entities that actually and legally possess or influence its operation.

Relevant to the legislative process in Poland concerning critical infrastructure is the Act of April 26, 2007 on crisis management, as amended, defining, among other things, the authorities competent in matters of crisis management and their tasks and rules of operation in this area, as well as executive acts issued on its basis. The introduced legal regulations definę both the concept of critical infrastructure, its protection and activitieś related to the prevention of crisis situations, response in the event of their occurrence and preparation to take control of them, as well as removal of their effects and restoration of key resources.

However, it should be emphasized that legal regulations on the protection of critical infrastructure have been placed not only in the above-mentioned law, but also in a number of legal acts covering various areas of state functioning. However, some legal acts do not directly refer to critical infrastructure (CI), and an analysis of the terms used, including those relating to facilities, indicates their similar and often even identical meaning. In this subject, such areas of activity as telecommunications activities, the production and trading of fuels and electricity, the performance of defense tasks by entrepreneurs, the creation of strategic reserves, the powers of the minister responsible for the State Treasure or the protection of persons and property are distinguished.[7]

Figure 2. Basic legal acts regarding critical infrastructure



Act of April 26, 2007 on crisis management (Journal of Laws 2007, No. 89, item 590, as amended)

Directive EC 2008/114/EC of December 8, 2008 on the identification and designation of European critical infrastructure

Regulation of the Council of Ministers of April 30, 2010 on the National Critical Infrastructure Protection Program (Journal of Laws of 2010, number 83, item 541)

Regulation of the Council of Ministers of April 30, 2010 on Critical Infrastructure Protection Plans (Journal of Laws of 2010, No. 83, item 542)

Regulation of the Council of Ministers of April 30, 2010 on the Report on National Security Threats (Journal of Laws of 2010, number 83, item 540)

Source: Romana Ł, Cygańczuk K., Prawny wymiar ochrony infrastruktury krytycznej – wybrane aspekty, Safety&Fire Technology, Vol. 59, Issue 1, 2022.

The legal act in force in Poland, on the basis of which certain systems are designated as European Critical Infrastructures (ECIs), is the EU Council Directive on the Identification and Designation of ECIs, which establishes a procedure for defining ECIs and the principles of a common EU approach to assessing the needs for improving the protection of such infrastructure, in order to better protect the population and minimize potential economic and social losses. The important element here is that these are such systems, the disruption or destruction of which would have a significant impact on two or more EU member states.

Taking into account the existing legal acts, it can be said that their scope regulates, among

[7] Romana Ł, Cygańczuk K., Prawny wymiar ochrony infrastruktury krytycznej – wybrane aspekty, Safety&Fire Technology, Vol. 59, Issue 1, 2022.

other things, the following issues in the area of operation and protection of critical infrastructure:

- preparing solutions in the event of destruction or disruption of critical infrastructure, including assisting the population in ensuring its survival conditions until the infrastructure is restored;
- working and maintaining critical infrastructure protection plans, including the resources necessary to perform the tasks included in them;
- ensuring the functioning of public administration in the event of an emergency and the ability to restore critical infrastructure;
- ensuring continuous monitoring of threats;
- procedures for carrying out tasks related to the protection of critical infrastructure, including responding to situations of destruction or disruption of its functioning and priorities for its protection and restoration;
- managing risks by identifying significant threats to critical infrastructure, including prioritizing responses to specific risks and identifying the forces and resources necessary to eliminate them;
- preparing and maintaining an inventory of facilities and systems that make up critical infrastructure;
- options for action in a situation of threats or disruption of critical infrastructure and its restoration;
- principles of cooperation between the public administration and owners and owners of intrinsic and dependent objects, installations or equipment of critical infrastructure in the field of its protection, including the principles of information transfer.

In addition to the above-mentioned legal acts, special attention has been paid to those elements of critical infrastructure that are important for ensuring the continuity of the state's functioning, regardless of the type of threats present. In view of this, other documents have also been issued, which in their provisions indicate the dimension in question in the area of critical infrastructure. These include:[8]

1. Order No 67 of the Prime Minister of October 15, 2014 on the organisation and operation of the Government Crisis Management Team, defining the mode and form of convening meetings and the rules of service and tasks of the team.[9]

2. Regulation of the Prime Minister of April 11, 2011 on the organisation and mode of operation of the Government Security Centre (RCB), defining the structure and tasks of the RCB [10]

3. Regulation of the Council of Ministers of September 21, 2018 amending the regulation on determining the government administration bodies that will establish crisis management centers and the manner of their operation.[11]

4. Act on organizing tasks for state defense carried out by entrepreneurs, which allowed for the creation of a legal structure for an entrepreneur of particular economic and defense importance, carrying out tasks for state defense (i.e. in the field of economic mobilization, militarization, operational planning, defense training, as well as those resulting from the host country's obligations państwa-gospodarza).[12]

5. Act on the Protection of Persons and Property - in the context of CI, the most important thing is that the above Act separates a category of areas, facilities, devices and transports subject to mandatory protection, important for defence, the economic interest of the state, public security and other important interests of the state (Article 5(2)). The Act also indicated the entities obliged to prepare lists of these installations (Article 5, section 3) and obliged the entities managing the installations to agree on their protection plans with the local provincial police commander (Article 7, section 1). The Act on the Protection of

[8] Romana Ł, Cygańczuk K., Prawny wymiar ochrony infrastruktury krytycznej – wybrane aspekty, Safety&Fire Technology, Vol. 59, Issue 1, 2022.
[9] M.P. 2014, item 926.
[10] https://www.gov.pl/web/rcb/o-rcb2.
[11] Journal of Laws 2018, item 1974.
[12] Journal of Laws 2001, No. 122, item 1320.

Persons and Property distinguished in detail elements of infrastructure of such importance (Article 5).[13]

6. Aviation Law Act - the act covers issues relating to air navigation, airport ground infrastructure and aircraft. A separate chapter (Articles 84–85) concerns rescue and fire protection at airports. Pursuant to Art. 84, the airport manager is obliged, among others, to: to develop an action plan in case of an emergency, organize and ensure the operation of a rescue and fire-fighting service equipped with specialized equipment, and maintain the necessary rescue and fire-fighting measures.[14]

7. Act on railway transport - the act applies to railway infrastructure, part of which is part of critical infrastructure. In this context, the act also defines the principles of railway infrastructure management, including: by maintaining it in a condition ensuring the safe operation of railway traffic (Article 5(1)(3)), as well as the obligation on the part of the manager to take actions to eliminate the threat in a situation where the safety of railway traffic or the safety of the transport of persons and goods is threatened (Article 5(5)). Moreover, for railway lines of state importance, the Act imposes on the Council of Ministers the obligation to determine their list by way of a regulation (Article 6(2)). At the same time, the minister responsible for transport is obliged to determine (in consultation with the Minister of National Defense) a list of railway lines of exclusively defense importance (Article 6(3)). The Act also contains provisions regarding the physical protection of railway infrastructure. Art. 59 section 1 provides for the creation of a railway security guard by one or more managers. Art. 60 section 1 of the Act specifies the tasks of this formation, indicating that it is, among others, responsible for the protection of human life or health, as well as property in the railway area, on trains and other railway vehicles. [15]

8. Telecommunications Law - the act regulates the principles of conducting business

[13] Journal of Laws 2005, No. 145, item 121.
[14] Journal of Laws 2006, No. 100, item 696.
[15] Journal of Laws 2007, No, 16, item 94.

involving the provision of telecommunications services. As a tool for protecting critical infrastructure, it is important for many reasons. It defines a telecommunications undertaking, which in many cases allows the installations, facilities and devices managed by it to be classified as being part of the critical infrastructure telecommunications system (Article 2, point 27). In this context, operators are obliged to submit to the President of the Office of Electronic Communications (UKE) and to make available to interested entities the technical specifications of the network terminations used, radio interfaces and their changes, before the telecommunications services to be provided using these network terminations or radio interfaces become available to users (Article 137(1)). From the point of view of critical infrastructure protection, Art. 178, 179 section 1 and 180f of the Act. Art. 178 section 1 indicates that "in the event of a particular threat", the President of UKE may, by way of a decision, impose specific obligations on telecommunications undertakings, taking into account the size of the threat and the need to limit its effects and the principle of minimizing the negative effects of the imposed obligations. In turn, Art. 179 obliges such entrepreneurs to perform tasks and obligations in the field of preparation and maintenance of specified network elements to provide telecommunications for the needs of the national security management system, including state defense, implemented on the principles specified in the plans, decisions and agreements concluded between these entrepreneurs and the interested entities.[16]

9. Water Law Act - the act comprehensively regulates water management issues and includes, among others: regulations regarding strict protection and supervision of specific areas, important from the point of view of providing drinking water, i.e. an element of critical infrastructure. It provides for the possibility of establishing protection zones for water intakes and protection areas for inland water reservoirs (Article 51, points 1-2). In the former, there are orders, prohibitions and restrictions on the use of water and land, and the protection zone itself is divided into direct and indirect protection areas (Article 52). In areas of direct protection, it is prohibited to use land for purposes unrelated to the

[16] Journal of Laws 2004, No. 171, item 1800.

operation of a water intake (Article 53), while in areas of indirect protection, restrictions may, but do not have to, apply to activities that reduce the usefulness of the abstracted water or the efficiency of the intake (Article 54). The above provisions create the possibility of additional protection of the critical infrastructure system relating to water supply.[17]

10. Act on Strategic Reserves - the Act defines critical infrastructure in a manner similar to the Act on Crisis Management. Article 3 of the Act indicates the essence of building strategic reserves - in this context, the following were mentioned, among others: threat to state security and defense, public security and order, support for the implementation of tasks in the field of state security and defense, restoration of CI, alleviating disruptions in the continuity of supplies serving the functioning of the economy and meeting the basic needs of citizens.[18]

11. Act of March 18, 2010 on special powers of the minister responsible for the State Treasury and their exercise in certain capital companies or capital groups operating in the electricity, crude oil and gas fuels sectors - this document replaced the Act of June 3, 2005 on the special powers of the State Treasury and their exercise in capital companies of significant importance for public order or public security. It refers to the protection of the CI section - strictly speaking, to the energy, energy raw materials and fuel supply system.[19]

12. Regulation of the Council of Ministers of June 24, 2003 on facilities that are particularly important for the security and defense of the state and their special protection - the regulation was issued on the basis of the Act on the general obligation to defend and specifies facilities that are particularly important for the security and defense of the state (§ 2). The extensive catalog, containing nineteen categories, includes, among others: facilities of formations and services (including the Police, the Internal Security Agency and the State Fire Service), facilities related to mineral extraction, telecommunications, state

[17] Journal of Laws 2005, No. 239, item 2019.
[18] Journal od Laws 2010, No. 229, item 1496.
[19] Journal of Laws 2010, No. 65, item 404.

reserve warehouses, dams and hydrotechnical devices, power plants and electrical energy facilities, as well as facilities subordinated to or supervised by Minister of National Defense. Pursuant to the regulation, these objects are subject to special protection (§ 5). They were also divided into objects of category I (listed in points 1-9 § 2) and objects of category II (listed in points 10-19 § 2). The Minister of National Defense is responsible for determining the requirements for preparing and conducting special protection of category I facilities, and the minister responsible for internal affairs has the same obligation in relation to category II facilities. In fact, facilities of both categories constitute, to a large extent, critical infrastructure, which is another example of the fact that its protection was prepared and carried out long before the decision was made about its legal and structural separation and additional requirements for its protection, which involve the need to prepare among others National Critical Infrastructure Protection Program. In addition to the above-mentioned legal acts, the Act of March 27, 2003 on spatial planning and development and the Act of September 4, 2008 on the protection of shipping and sea ports should also be mentioned. They are also related to the issues of critical infrastructure. The first one requires that the needs of state defense and security be taken into account in spatial planning and development (Article 1(2)(8)), while the second one regulates issues of protection, among others. seaports and port facilities (Article 2(1)).[20]

[20] Journal of Laws 2003, No. 116, item 1090, Journal of Laws 2003, No. 80, item 717, Journal of Laws 2008 No. 171, item 1055.

2. Characteristics of critical infrastructure systems and their socio-economic functions.

Critical infrastructure systems (CIS) perform key socio-economic functions, ensuring the stability, security and comfort of society. The characteristics of each system and its functions will be presented below.

Energy, energy resources and fuel supply system. The provision of electricity and heat to citizens, as well as the supply of fuels to state structures, guarantees the functioning of the economy and society. The energy needs of the economy and society make the system of supply of energy, energy raw materials and fuels a system of particular importance for the functioning of the state. The system's infrastructure ensures the extraction of coal for the electric power industry, the generation of electricity with its supply to individual consumers and industry, enables the extraction, import and processing of crude oil and the production and supply of liquid fuels for spheres of state activity that use them, as well as the extraction, import and supply to consumers of natural gas that guarantees the use of household heating appliances and the production of material goods based on natural gas.

Communications system. Communications systems provide for the transmission of information and include mail and telecommunications, as well as broadcasting. By telecommunications we mean the transmission, reception or transmission of information, of whatever kind, by means of wires, radio waves or optical waves or other means using electromagnetic energy. Communications are of critical importance in the economy for business processes, management, or in administration-citizen-citizen-administration relations, as well as between citizens themselves. Nowadays it is difficult to imagine an information society without effective transmission of information.

ICT network system. According to the definition contained in the Act of July 18, 2002 on the provision of services by electronic means (Journal of Laws No. 144, item 1204, as amended), an ICT system is a set of cooperating IT devices and software, providing for the processing and storage, as well as sending and receiving data via telecommunications networks by means of a terminal device appropriate for the type of network. On the other hand, under the term telecommunications network, as defined in Article 2(35) of the July 16, 2004 Law. - Telecommunications Law (Journal of Laws No. 171, item 1800, as amended), should be understood as transmission systems and switching or routing devices, as well as other resources that enable the transmission, reception or transmission of signals by wire, radio waves, optical waves or other means using electromagnetic energy, regardless of their type. The operational capacity of ICT systems, therefore, understood as a set of devices and software, capable of working together to process collected data, is achieved only when these devices are connected via a telecommunications network. Their role is to transmit information, ensuring the effective implementation of the other two features of ICT systems, namely sending and receiving data.

Public administration bodies to perform their statutory duties, use:

- ICT systems dedicated to the processing and collection of various data,
- physically or logically separated telecommunications networks owned by public administration bodies or leased from telecommunications network operators. In this regard, the public administration uses the services of leased telecommunications networks of telecommunications entrepreneurs.

The totality of ICT systems existing and operated by the public administration, interconnected internally by means of telecommunications networks, is included in the Law on Emergency Management under the concept of ICT network systems, which are one of the components of the state's critical infrastructure.

Financial system. The financial system is a set of legal norms and a set of financial institutions whose task is to collect, divide and spend the state's monetary resources. A well-functioning financial system is crucial for the smooth functioning of the state and society. The public administration body exercising state supervision over the financial market in Poland is the Polish Financial Supervision Authority (PFSA).

The financial system consists of several segments:

1. budgetary – all legal norms and organizational structures regulating the functioning of the state budget and local government units. The state budget finances all activities aimed at fulfilling the state's statutory obligations towards citizens;

2. banking - all legal standards regulating the conduct of banking activities, the establishment and organization of banks, branches and representative offices of foreign banks, as well as branches of credit institutions and prudential standards established by the Polish Financial Supervision Authority. The central bank of the Republic of Poland, the National Bank of Poland (NBP), plays a fundamental role in the banking subsystem. The NBP performs three basic functions: a) an issuing bank - the NBP has the exclusive right to issue currency which is legal tender in Poland, b) a bank of banks - the NBP performs regulatory functions in relation to banks, which are aimed at ensuring an efficient and effective payment system, and stability of the banking sector, c) central bank of the state - NBP provides banking services to the state budget, maintains bank accounts of the government and central state institutions, state special funds and state budgetary units and executes their payment orders;

3. insurance – regulates the creation, division and organization of the insurance market. Insurance is divided into two categories: a) social insurance - aimed at preventive and insurance protection of health, ability to work and life of the population, it is compulsory and universal. The most important links in the social insurance subsystem are the Social Insurance Institution (ZUS). ZUS is a state public law institution that carries out tasks in the field of social insurance in Poland. Currently, approximately 25 million customers use ZUS services. The resources of the Social Insurance Fund, administered by ZUS, constitute nearly 60% of the state's monetary resources, Open Pension Funds (OFE) and the Agricultural Social Insurance Fund (KRUS); b) life, personal and property insurance - this type of insurance activity is performed by insurance companies based on permits from the supervisory authority. An insurance company may conduct insurance activities only in the form of a joint-stock company or a mutual insurance company.

4. capital - where medium and long-term financial instruments are traded (e.g. shares and bonds). Trading takes place mainly on the Stock Exchange (WSE). The Warsaw Stock Exchange is a joint-stock company established by the State Treasury. The State Treasury holds a 35% share in the Company's share capital, which constitutes a 51.40% share in the total number of shareholder votes. The State Treasury is the only shareholder holding more than 5% of the total number of votes. In addition to the WSE, important participants in the capital segment include: The Central Securities Depository of Poland, BondSpot S. A. (joint-stock company operating the Polish over-the-counter market), brokerage houses and offices, and investment fund companies.

Food supply system. The food supply system is a field of the economy that includes the production of production resources (e.g. fertilizers, feed) and services for agriculture, the production and acquisition of food raw materials (in agriculture, fishing, forestry, hunting), the purchase of food raw materials and their storage. and transport, processing of food raw materials, trade in food products (warehousing and storage of food, wholesale and retail trade, export and import) and the food safety system covering all components of the food supply chain.

The food supply system is one of the basic pillars of the national economy, which has a direct impact on the economic security of the state. The strategic goal of this system is to ensure the nutrition of the nation by maintaining the production capacity of the food economy ensuring food security, food and feed safety.

Food security is one of the basic needs of society. It is caused by a number of factors and is a much more complicated issue than producing a sufficient volume of food. Also important are: access to food for poor people, agricultural systems, agricultural policy, international trade policy, food costs, food diversity and safety, food chains, distribution, nutritional value and health issues. An important element of food security is ensuring society has access to sufficient food.

Food security should be treated on an equal footing with other strategic state functions, such as ensuring energy security, environmental security, and security of water resources, a necessary condition of which is maintaining agricultural production at an appropriate level (including readiness to conduct production by maintaining land in good agricultural condition), as well as creating appropriate conditions for this production (through support mechanisms and other agricultural policy instruments).

Agriculture is one of the most important elements of the food supply system and clearly affects the country's economic security in the production dimension (production and processing volume), which determines the possibility of ensuring the country's food security and supporting the Armed Forces. The goals of agriculture in the context of food security are: maintaining and increasing productivity in the future, maintaining the production base, i.e. agricultural land ready for production, and reducing the burden on the environment. Food security, due to its transnational nature, is the goal of both national and Community agricultural policy.

The main component of the food supply system is the production and procurement of food raw materials. It primarily includes matters relating to:

- crop production and crop protection,
- seeding, excluding forest reproductive material
- animal production and animal breeding.

The main objective of action in this area should be to maintain agricultural production, processing and distribution capacity at a level ensuring the supply of society with at least basic agri-food products (meat, dairy, cereal products and sugar). It is necessary to create conditions for restoring and maintaining agricultural and livestock production (plants and animals) in the event of events that limit this production (natural and industrial disasters, acts of terror, war). It should be emphasized that agricultural production and the method of its distribution determine the proper nutrition of the population (providing the appropriate calorific value and amount of nutrients), and, constituting the basic production link in the entire production cycle, it is also an important element of the national economy.

The food supply system also covers:

- agri-food processing and storage,
- commercial quality of agricultural and food products,
- mechanisms for regulating agricultural markets.

Water supply system. The water supply system is the interconnected enterprises and devices that collect, refine, supply and purify water for the population and industry. As a result of the increasing concentration of population in urban centers, water supply and sewage collection have become one of the most important services ensuring the efficient functioning of communities. The importance of water supply is not limited only to urban areas, rural areas also use significant amounts of water for plant and animal production.

Health care system. The health care system is a set of people and institutions whose task is to provide health care to the population, and its efficient functioning (together with the rescue system) is a guarantee of citizen's rights enshrined in the Constitution. System participants can be divided into the following categories:

- beneficiaries – i.e. patients,
- health insurance institution acting as a payer - i.e. the National Health Fund (NFZ),
- healthcare providers: entities performing medical activities, in accordance with Art. 4 and 5 of the Act of April 15, 2011 on medical activities (Journal of Laws of 2011, No. 112, item 654, as amended),
- control and supervision bodies: the State Sanitary Inspection, the State Pharmaceutical Inspection, the Patient Ombudsman, voivodes and their provincial public health centers and provincial consultants in individual medical specialties,
- The Ministry of Health, which sets the directions of the country's health policy and has control powers, as well as national consultants working with it in individual medical specialties.

The most important elements in terms of system availability are medical entities and the

National Health Fund. Stationary health care is provided in general hospitals and other medical entities.

Transport system. Transport should be understood as the movement of people and loads (object of transport) in space using appropriate means of transport. The movement of goods, people and services is one of the basic characteristics of the modern economy and society, which is why an efficiently functioning transport system is one of the pillars of a modern state.

Generally, transport can be divided into passenger transport (communication) and freight transport (cargo). Moreover, depending on the type of transport, it is divided into:

- railway transport,
- car transport,
- air transport,
- pipeline transport,
- inland navigation
- shipping.

Rescue system. Rescue should be understood as all organizational measures and undertakings undertaken to save health and life, property and the environment in danger, as well as to predict, recognize and eliminate the effects of events. Together with health care systems, they constitute the basis for the implementation of citizens' constitutional rights to protect their life and health.

The Rescue System in Poland includes:

- National Rescue and Firefighting System - the purpose of its operation is to save life, health, property and the environment. This system brings together fire protection units, other services, inspections, guards, institutions and entities that voluntarily, through a civil law agreement, agreed to cooperate in rescue operations.

- State Medical Rescue - system, established to save human life and health. The units of the system are: hospital emergency departments, medical rescue teams, including air medical rescue teams.
- Emergency Notification System - is currently being established to integrate the National Rescue and Firefighting System and the National Medical Rescue System.
- Mountain Rescue - activities related to carrying out rescue operations in mountainous terrain, searching for missing persons, providing medical assistance to accident victims, transporting the injured to places where they can be provided with full medical assistance; also preventive activities related to information about hazards, danger of avalanches and expected weather breakdowns. Mountain Rescue is organized on the basis of the organizational structures of the Mountain Volunteer Search and Rescue and Tatra Volunteer Search and Rescue.
- Maritime rescue - the activity of saving life and property at sea. In Poland, marine rescue is primarily handled by two state institutions: the Maritime Search and Rescue Service (known as the SAR Service), the Navy.
- Mine rescue dealing with providing assistance to miners and mines in danger, as well as removing the consequences and restoring safe working conditions after the occurrence of these hazards, and preventive and training activities in mines. Each mine has its own rescue squad, however, the main base of mine rescuers in Poland is the Central Mine Rescue Station, based in Bytom, along with district rescue stations.
- Water rescue - the carrying out of rescue activities, consisting in particular of organizing and providing assistance to people who have suffered an accident or are at risk of losing their life or health in an aquatic area.
- National Contamination Detection and Alert System (NDSDS) - is a specialized subsystem for countering and eliminating chemical, biological, radioactive and nuclear contamination.

A system to ensure the continuity of public administration. Public administration is the power to perform tasks assigned by the legal order to the state and its organs or other entities performing power functions. Public administration in Poland consists of, among others: government administration and local administration.

Government administration can be divided, depending on the scope of its activities, into government administration at the central level (the Prime Minister, the Council of Ministers, ministers and central government administration bodies) and government administration at the voivodeship level (the representative of the Council of Ministers in the voivodeship is the voivode, government at this level includes bodies of consolidated government administration and bodies of non-integrated government administration).

Local government administration in Poland is formed at three levels: commune, district and voivodeship. Local government bodies include:

- decision-making bodies: province assembly (16 provinces), county council (308 terrestrial counties and 65 urban counties - cities with county rights), municipal council (2489 - municipalities);
- executive bodies: provincial board, district board, mayor (mayor, city president).

The system of production, storage, storage and use of chemical and radioactive substances, including pipelines of hazardous substances. The development of the chemical sector is determined by its specificity - it is the raw material base of all sectors of the economy. Chemical production is replacing products made of metal, wood, glass and natural fibers. The largest recipients of chemical industry products are the following sectors: machinery and metal, automotive, electrical engineering and electronics, construction, paper and printing, textile and clothing, and agriculture. Domestic production does not meet the demand for chemicals. The chemical industry branches include:

- Large chemicals - cheap products and mass-used in large quantities: petrochemical industry, soda industry, sulfuric acid industry, artificial fertilizers industry, plastics industry, artificial fibers industry.
- Low-volume chemicals - expensive products and used in small quantities: pharmaceutical

industry, cosmetics industry, auxiliary products industry - cleaning, hygiene and plant care products, etc..

- Chemical processing - which produces final products based on large-volume products: rubber industry, plastics processing industry, paints and varnishes industry, distribution and trade of reagents.

The Radioactive Waste Disposal Facility is responsible for the collection, transport, processing and storage of waste generated by all users of radioactive materials in the country. The place where radioactive waste generated in Poland is stored is the National Radioactive Waste Repository (ZUOP). The landfill in Różan has existed since 1961 and is the only facility of this type in our country. The National Atomic Energy Agency maintains and verifies a register of closed radioactive sources. It includes information about over 16,000. sources, including spent radioactive sources. The national system of records of nuclear materials fulfills the function of control over these materials in Poland

In Poland, apart from oil pipelines (crude oil, final products) and natural gas, there are no pipelines transporting hazardous substances.

3. The National Critical Infrastructure Protection Program, Plans for the protection of critical infrastructure.

National Critical Infrastructure Protection Program (NPOIK) was adopted by a resolution of the Council of Ministers on March 26, 2013 and updated in 2023. It was developed under Article 5b (1) of the Law on Emergency Management. The first edition of the Program established a framework for multilateral partnerships for uninterrupted access to services that ensure the maintenance of a certain standard of living and enable proper relations between the state and the citizen. Access to such services is crucial to the smooth functioning and development of a modern state, society and economy. These services and the infrastructure providing them have been referred to as critical infrastructure, which has already been defined in Chapter 1.

The National Critical Infrastructure Protection Program covers CI included in the unified list of facilities, installations, equipment and services included in critical infrastructure by system, as referred to in Article 5b (7)(1) of the Law on Emergency Management.

It should be noted that the NPOIK takes into account international agreements to which the Republic of Poland is a party, in particular the Republic of Poland's membership in the European Union, the North Atlantic Treaty Organization, the Organization for Security and Cooperation in Europe and other international organizations.

The goal of the NPOIK is to create conditions for improving the security of critical infrastructure, which, together with other program documents, will translate into the overarching goal of increasing the security of the Republic of Poland. Achievement of the Program's goal will be made possible through the following intermediate goals:

- acquiring a specific level of awareness, knowledge and competences of all Program participants regarding the importance of CI for the efficient functioning of the state and the ways and methods of its protection,

- introduction of a risk assessment methodology that takes into account the full range of threats, including a methodology for dealing with threats with very low probability and catastrophic consequences,
- introducing a coordinated and risk-based approach to the implementation of CI protection tasks,
- building partnership between participants of the CI protection process,
- introducing mechanisms for the exchange and protection of information transferred between participants of the CI protection process.

To enable the achievement of the above Program objectives, **priority actions have been defined for a period of 2 years** from the adoption of the Program update by the Council of Ministers - they are as follows:

1. deepening cooperation between Program participants in the area of CI protection,
2. identification of dependencies between CI systems,
3. assessing the risk of disruption of the functioning of the CI system.

The Crisis Management Act adopts a **sanction-free approach to the protection of critical infrastructure**. Its basis is the assumption that increasing the effectiveness of CI protection can only occur through the actions of its operators supported by the capabilities and potential of public administration. CI operators have the best knowledge and tools to reduce threats to their operations. They are also able to make the most appropriate choice of strategy to minimize the effects of these threats. In an attempt to maintain a balance between the authoritative influence of the state and the expenses necessary to improve CI security, the Crisis Management Act does not provide for sanctions for failure to fulfill the obligations specified therein, and does not provide for budget support for CI operators

As a result, in order to achieve the objectives of the Program, it is necessary to adopt principles that should be followed by its participants. **The most important principles of the Program were**:

- co-responsibility understood as a common (collective) desire to improve CI security resulting from the awareness of its importance for the functioning of both public administration bodies and CI operators, society, the economy and the state;
- cooperation, which means that CI protection participants perform specific, convergent and mutually complementary tasks together to achieve a common goal resulting from the principle of shared responsibility; it is necessary to avoid duplication of activities and costs incurred and to use the available forces and resources more effectively;
- trust understood as the belief that the motivation of CI protection participants (this applies in particular to the administration and CI operators) is to pursue a common goal, which is to improve the security of CI and RP.

In addition, the following rules will also apply to the Program:

- proportionality and risk-based action;
- recognizing the differences between CI systems;
- the leading role of the minister responsible for the CI system;
- equality of CI operators;
- complementarities.

The addressees of NPOIK are in particular government administration and CI operators:

- The main addressees of the Program in government administration are ministers responsible for CI systems and voivodes. However, taking into account the breadth and cross-section of the administration's activities, the Program is also addressed to other administrative bodies, institutions and entities. It is a source of information on CI protection activities and opens opportunities to engage in its implementation and establish effective cooperation with ministers responsible for CI systems and CI operators.
- In the case of CI operators, the program is addressed primarily to their management. Each operator of the newly designated CI automatically becomes the addressee of the Program. CI Operator, in accordance with § 1 of the Regulation of the Council of Ministers of April

30, 2010 on the National Critical Infrastructure Protection Program (Journal of Laws No. 83, item 541), is the owner and independent and dependent holder of facilities, installations, devices and services critical infrastructure. CI operators, in accordance with Art. 6 section 5 of the Crisis Management Act, they are obliged to protect it.

It should be emphasized, however, that the provisions of the Program may be used by all those who consider the Program helpful in the process of increasing the resistance to disruptions of their own infrastructure, including local government bodies and private entities that are not CI operators. The Program is also addressed to those who, following the principles of the Program, would like to get involved in the process of achieving its goals.

NPOIK, based on three basic principles, opens many new opportunities in the field of scientific research and implementation-oriented development work. The presentation of actions taken by the administration to increase the level of CI security is intended to serve as a guide for the scientific community to develop tools helpful in the implementation of the Program.

Every citizen depends on the delivery of services provided using CI. Knowledge regarding actions taken by the administration to increase the level of CI security (and therefore all of us) requires dissemination. The program presents solutions and good practices in the field of protection, enabling their application in everyday life, which may be useful in increasing individual resistance to threats.

A key stage of the CI protection process is the identification of objects, devices, installations or services whose destruction or disruption of functioning could cause a crisis situation. In order to ensure maximum objectivity, the Government Center for Security, in cooperation with ministers and heads of central offices and with the support of private entrepreneurs, has developed CI identification criteria. The criteria are divided into two groups:

- system criteria - characterizing quantitatively or subjectively the parameters (functions) of a facility, device, installation or service, the fulfillment of which may result in being classified as critical infrastructure. These criteria are presented for each CI system,

- cross-cutting criteria – describing parameters relating to the effects of destruction or cessation of operation of a facility, device, installation or service. Cross-cutting criteria include: human casualties, financial impact, need for evacuation, loss of service, reconstruction time, international impact, uniqueness.

The criteria define numerical values used to characterize the feature due to which a given infrastructure is classified as CI. If this is not possible, the functions performed by the tested infrastructure are described.

CI identification was divided into three stages:

1. first selection of objects, installations, devices or services that could potentially be recognized as CI in a given system, system criteria appropriate for a given CI system should be applied to the system infrastructure,

2. verifying that the facility, equipment, installation or service plays a key role in the security of the state and its citizens, and that it serves to ensure the smooth functioning of public administration bodies, as well as institutions and entrepreneurs, the definition in Article 3(2) of the Crisis Management Law should be applied to the infrastructure identified in stage one,

3. assessment of the potential effects of the destruction or cessation of functioning of potential CI, cross-cutting criteria should be applied to the infrastructure selected in the first and second stages, and the potential CI must meet at least two cross-cutting criteria.

The coordinator of the implementation of the National Critical Infrastructure Protection Program is the Director of the Government Center for Security (RCB). In cooperation with all interested parties, guided by the principles of the Program, RCB will implement the provisions of the Program. The Director of the RCB, taking into account information received from the ministers responsible for CI systems and voivodes, presents an annual assessment of the Program's effectiveness at the meeting of the Council of Ministers.

Moreover, taking into account the fact that the Government Security Center is the national contact point for the institutions of the European Union and the North Atlantic Treaty Organization and their member countries in the field of protection of critical infrastructure and European critical infrastructure, it will coordinate in the country the regulations, decisions and obligations undertaken by the Republic of Poland regarding CI protection.

In terms of subject matter, the action plan in the 2-year period after the Council of Ministers adopted the NPOIK update covers the following groups:

1. organizational and legal activities,
2. technical activities,
3. educational and training activities.

As part of the organizational and legal activities, the following were identified:

- development of procedures for conducting internal controls and audits (leading: RCB, supporting: CI system coordinators + CI operators);
- development of a methodology for assessing the risk of disruption of CI functioning and identifying dependencies between CI systems (leading: RCB, supporting: CI system coordinators + CI operators);
- development of a communication procedure in the event of threats to CI (leader: RCB, supporting: CI system coordinators + CI operators).

Technical activities include:

- launching working groups to develop minimum standards for ensuring CI security (leading: RCB, supporting: CI operators);
- verification of the effectiveness of the methodology for identifying CI objects (leading: RCB, supporting: CI system coordinators + CI operators);
- launching a database of incidents in CI facilities (leading: RCB, supporting: voivodes + CI operators);

- launching a training platform for CI operators and public administration (leader: RCB).

In turn, educational and training activities include:

- development of a basic training program in the field of CI protection and preparation of teaching materials for self-education for CI operators and public administration (leading: RCB, supporting: CI system coordinators + CI operators);
- developing and publishing information brochures and guides on CI protection for CI operators and public administration (leading: RCB + CI system coordinators, supporting: CI operators);
- conducting pilot exercises in the field of CI protection in one of the CI facilities (leading: RCB, supporting: coordinator of the selected CI system + CI operators).

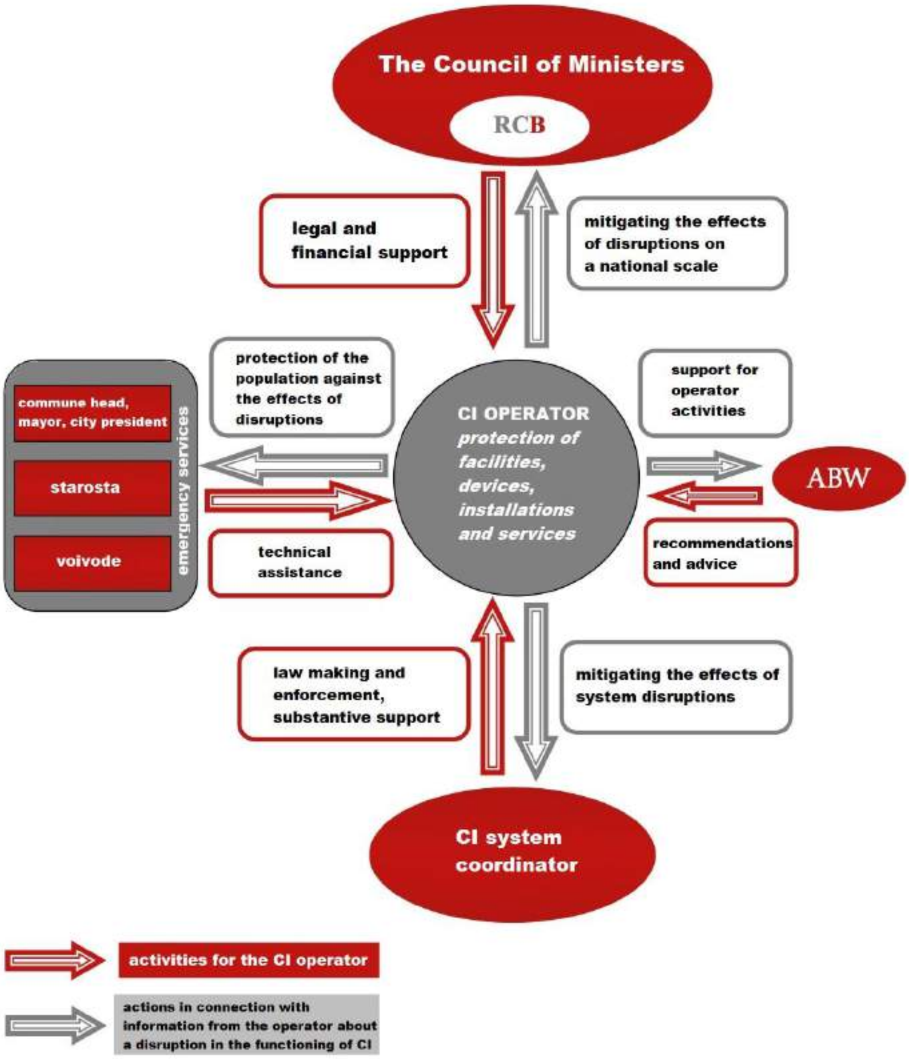
CI protection activities are financed from the Program participants' own funds and planned in their budgets: in the case of administration, pursuant to Art. 26 section 1 and 2 of the Crisis Management Act, and in the case of CI operators, pursuant to Art. 6 section 5 above Act.

4. Institutions and bodies responsible for the preparation and implementation of the National Critical Infrastructure Protection Program.

Determining the division of competences of the participants of the National Critical Infrastructure Protection Program, understanding the role and responsibility of each of them in the system of protecting the critical infrastructure of the Republic of Poland is the basis for the effectiveness and sustainability of the efforts undertaken in this area and will contribute to achieving the objectives of the Program.

The implementation of the Program requires the involvement of all possible interested parties, however, the main effort rests, in accordance with their competences, on the Government Security Center, ministers responsible for CI systems and operators of critical infrastructure, specified in the list of critical infrastructure. The Crisis Management Act defined the basic obligations of entities involved in CI protection. The obligations of the authorities arising from other provisions of the Act, especially in the context of including CI protection tasks in crisis management plans, have remained unchanged.

Figure 3. Main entities participating in the CI protection process and their roles


The Council of Ministers
RCB
legal and financial support
mitigating the effects of disruptions on a national scale
protection of the population against the effects of disruptions
CI OPERATOR
protection of facilities, devices, installations and services
support for operator activities
ABW
recommendations and advice
commune head, mayor, city president
starosta
voivode
emergency services
technical assistance
law making and enforcement, substantive support
mitigating the effects of system disruptions
CI system coordinator
activities for the CI operator
actions in connection with information from the operator about a disruption in the functioning of CI

Source: National Critical Infrastructure Protection Program – consolidated text, 2023.

In the field of critical infrastructure protection, **the Government Center for Security** carries out the tasks specified in Art. 11 section 2 point 11 of the Act on Crisis Management and its implementing acts. As part of the implementation of the above tasks, the Government Center for Security, playing the main role in building a critical infrastructure protection system based on shared responsibility, cooperation and trust, as well as on the other principles of the Program, will implement the activities provided for in the action plan, listed in Chapter

3, as well as among others:

- build partnerships between all interested parties and support and facilitate this process at lower levels,
- build, maintain and develop an information exchange network between Program participants,
- support ministers and heads of central offices in assessing the risk of a crisis situation caused by a disruption in the functioning of the CI system,
- develop, disseminate and implement tips, recommendations and guidelines for managing the risk of CI disruption,
- develop mechanisms to support the reconstruction of CI,
- support the creation (where justified) of structures to increase close cooperation between the private sector and public administration at all levels to maintain the effectiveness of the Programme,
- publish information on good practices in the area of CI protection and facilitate their exchange,
- initiate and support scientific research and development work related to CI protection,
- promote educational programs and activities aimed at raising awareness in the area of CI protection,
- conduct training in the area of CI protection and support their organization,
- evaluate the effectiveness of the Program.

In turn, **CI operators** have the best knowledge and conditions to limit threats to CI, reduce its susceptibility to these threats and select the most appropriate strategies to minimize the effects of these threats. Pursuant to the Crisis Management Act, they are entrusted with the obligation to protect critical infrastructure facilities, devices, installations and services. Therefore, they are obliged to:

- preparation and implementation, in accordance with anticipated threats, of critical infrastructure protection plans and maintaining own reserve systems ensuring security and maintaining the functioning of this infrastructure until it is fully restored,
- appointing a person responsible for maintaining contacts with entities responsible for the protection of critical infrastructure,
- immediate submission to the Head of the Internal Security Agency of information regarding terrorist threats to critical infrastructure,
- cooperation in the creation and implementation of the Program.

The person(s) in charge of maintaining contact with entities competent for the protection of critical infrastructure should receive/transmit information on threats to the CI in question and have the technical capacity to perform this task on a 24-hour basis. It should also have as much knowledge as possible about the operator's critical infrastructure and its operation. Accordingly, CI operators also participate in CI protection activities by:

- active cooperation with public administration (at all levels) and other CI operators,
- support for public administration (at all levels) with expert knowledge regarding the functioning of CI in the planning process in the event of a crisis situation,
- exchanging information on threats with other CI operators,
- improving skills and ability to respond to crisis situations, including through appropriate education and organization of staff exercises,
- providing public administration and other CI operators with knowledge about the dependencies and interdependencies between their own CI and CI operating in other sectors of the economy,
- identification of best practices and standards that can help protect CI,
- participation in the promotion of educational programs and training in the field of CI protection,
- participation in exercises on crisis management and CI protection.

Another group responsible for the preparation and implementation of NPOIK are **the ministers responsible for critical infrastructure systems**, who play an important role in the CI protection system. Their work is a guarantee of the involvement of the highest state authorities in the process of building state security. Taking into account the adopted CI protection model, each CI system needs a coordinator with the best knowledge about it, understanding its structure and the needs of the entities involved. Ministers responsible for government administration departments or task areas comparable to CI systems are best prepared to perform this role on the part of the administration. Recognizing the differences between CI systems, in accordance with the requirement imposed by the Crisis Management Act, the Program identifies ministers responsible for individual systems.

Within the meaning of the Program, the responsibility of ministers for the CI system consists in particular in:

- supporting RCB in building a critical infrastructure protection system based on shared responsibility, cooperation and trust, as well as other principles of the Program;
- cooperation with RCB and support in identifying CI and implementing and updating NPOIK;
- initiating changes to legal acts in order to facilitate and support the performance of CI protection tasks;
- assessing the risk of disruption of the functioning of the CI system caused by destruction or disruption of the functioning of CI;
- cooperation with bodies whose competences include matters relating to components (elements) of the CI system that are not directly within the competence of the coordinator;
- cooperation with other CI system coordinators in terms of dependencies between CI systems;
- cooperation with operators of critical infrastructure in terms of its protection, animating and maintaining this cooperation;

- organization and operation of the system CI protection forum and participation in the CI protection mechanism to the extent described in the Program;
- support for the organization of systemic exercises assessing the efficiency of CI protection;
- support for activities aimed at recreating CI;
- performing periodic analyzes and assessments of the effectiveness of critical infrastructure protection in the appropriate system;
- inspiring the implementation of modern CI protection techniques in the system;
- organizing training, conferences and scientific and research symposia, improving organizational, technical and formal and legal measures to counteract disruptions in the functioning of critical infrastructure;
- stimulating the activity of entities involved in the CI protection process within the system;
- advice and assistance for CI operators and public administration;
- supporting systemic initiatives aimed at improving the security of CI operation);
- agreeing on CI protection plans included in the CI list within a given system.

Moreover, guided by the principles of the Program, ministers responsible for the critical infrastructure system:

- participate in the preparation and promotion of strategies prepared at the central level aimed at encouraging the private sector to participate in the Program,
- prepare strategies aimed at encouraging the private sector to participate in the Program,
- build partnership between interested parties within the CI system,
- promote educational programs in the field of CI protection at the level of the CI system,
- organize CI protection training for local governments and private sector partners as part of the CI system,
- promote activities aimed at raising awareness in the area of CI protection,

- implement a business continuity management system for the offices serving them,
- ensure that tasks related to CI protection are taken into account in the activities of the bodies subordinated to them.

When creating policy within the CI system, ministers responsible for the systems cooperate closely with entities competent in a given area. If responsibility for the system has been divided between more than one minister, each coordinator will carry out the above-mentioned tasks in relation to those facilities that have been agreed with the other co-coordinators.

Moreover, **other public administration bodies** are also involved in the process of preparing and implementing NPOIK, not necessarily directly, but they constitute important elements supporting/supplementing the CI system. These include entities such as:

1. The President of the Republic of Poland - although he is not directly involved in tasks for CI protection, due to his competences in the area of state security, he is an important element of the CI protection system. It guarantees the involvement of the highest state authorities in the process of improving the security level of CI and, therefore, the state. The President of the Republic of Poland participates in the Program within the scope of his constitutional competences covering national security and defense. It supports central and local government administration in activities aimed at protecting CI and aiming to achieve the objectives of the Program.

2. Council of Ministers - exercises executive power and manages government administration. The tasks of the Council of Ministers concern all areas of the political, economic, social and cultural life of the state, including ensuring the internal and external security of the state and public order. The Council of Ministers, by adopting the NPOIK resolution, gives impetus to activities aimed at achieving its goals implemented by its subordinate bodies and entities, as well as through the functioning of the Government Crisis Management Team.

3. Ministers and managers of central offices performing tasks in the field of crisis management - their role is to support with knowledge the activities of the involved parties to achieve the Program objectives, participate in the process of assessing the risk of a crisis situation in the country caused by disruption of the functioning of the CI system, cooperation with relevant entities in matters of CI protection in the field of information exchange, good practices, scientific research and development programs and others, and performance of tasks specified in the Crisis Management Act.

4. Voivodes – play an important role in the system of critical infrastructure protection and crisis management. Pursuant to the applicable legal acts, the task of voivodes and organizational units responsible for crisis management in the voivodeship office is: organizing the implementation of tasks in the field of critical infrastructure protection resulting from its location in the territory of the voivodeship, including including these tasks in the voivodeship crisis management plans, collecting and processing information regarding critical infrastructure located in the voivodeship, providing, if there is a need resulting from the voivodeship crisis management plan, the necessary information on critical infrastructure in the voivodeship to the competent public administration body operating in this area and agreeing on the critical infrastructure protection plans of CI operators.

5. Special services – fulfill a specific role in CI protection. They have at their disposal developed forces and means to identify threats caused by intentional human activity. The exchange of information about these threats with CI operators and other entities competent in CI protection matters in the manner specified by law and internal procedures, to the extent permitted by the provisions on the protection of classified information, is crucial in the CI protection planning process. A special role has been assigned to the Internal Security Agency. Pursuant to Art. 12a of the Crisis Management Act, the head of the Internal Security Agency, in the event of receiving information about the possibility of a crisis situation resulting from a terrorist event threatening critical infrastructure, human life or health, significant property, national

heritage or the environment, may provide recommendations to the bodies and entities at risk. these activities and provide them with the necessary information to counteract threats. The head of the Internal Security Agency informs the director of the Central Security Agency about the above activities and supports public administration bodies in activities related to the prevention, counteracting and removal of the effects of terrorist events. Public administration bodies are obliged to immediately provide the Head of the Internal Security Agency with information in their possession regarding terrorist threats to critical infrastructure.

6. Chief administrative officers, commune heads, mayors and city presidents - due to the fact that critical infrastructure is physically located in communes, cities and poviats. Therefore, chief administrative officers,_commune heads, mayors and presidents of cities and the services subordinated to them play an important role in the protection of the population exposed to the potential effects of disruption of the functioning of CI and in the protection of CI, enabling direct and fastest support for its operators.

7. Scientific environment - for the implementation of the Program it is necessary to develop tools enabling more effective operation of all interested parties. Scientific units and the community are a source of knowledge in this area and provide expert support to Program participants.

5. Security and protection services in the Critical Infrastructure security management system.

Critical infrastructure protection should be understood as a process of ensuring its security:

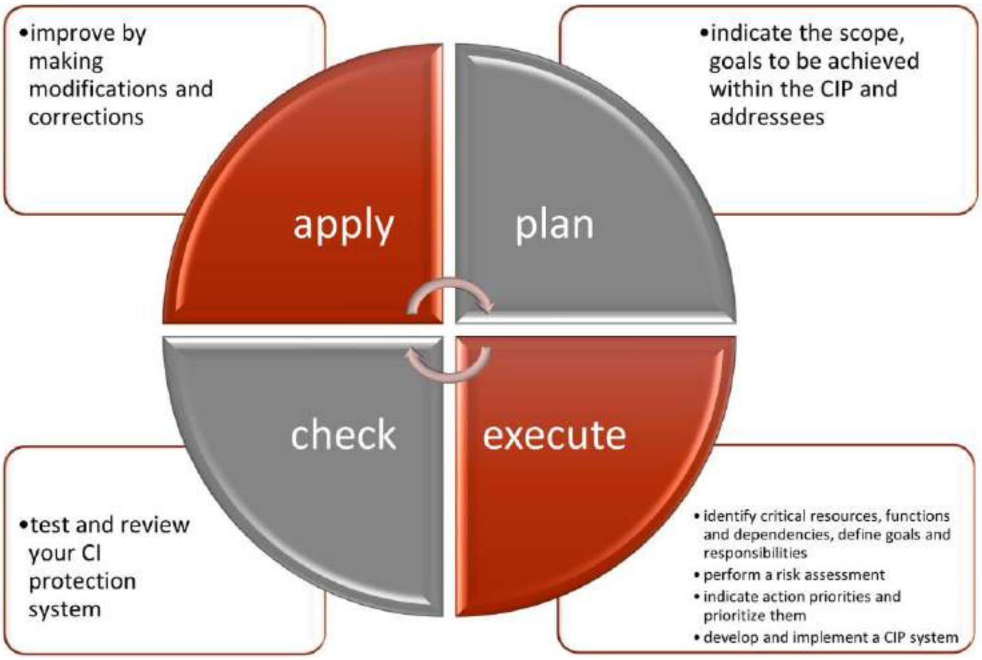
- taking into account achieving the expected result and continuous improvement,
- covering a significant number of task areas and competencies,
- involving many interested parties,
- covering all activities aimed at ensuring the functionality, business continuity and integrity of critical infrastructure.

The critical infrastructure protection process understood in this way consists of the following stages:

1. indication of the scope, goals to be achieved within CI protection and the addressees of these activities,
2. identification of critical resources, functions and determination of the network of connections (dependencies) with other CI systems, including entities and bodies,
3. defining the roles and responsibilities of those participating in the CI protection process,
4. risk assessment,
5. indication of action priorities and their prioritization depending on the results of the risk assessment,
6. development and implementation of a critical infrastructure protection system, including the development and acceptance of CI protection and restoration plans,
7. testing (through exercises) and review (through audit and self-assessment) of the CI protection system and measuring progress towards achieving the goal,
8. improvement, understood as introducing modifications and corrections as a result of tests, reviews and measurements.

The need for continuous improvement allows the CI protection process to be included in the Deming cycle. Incorporating the CI protection process into a cycle allows, after measuring the effects, to take improvement or corrective actions at the stage at which a deviation from the expected results was found. It is also possible to redefine goals. Subsequent repetitions of the cycle should bring you closer to achieving them. The Deming cycle is applicable at each level at which CI protection takes place and should be repeated at established intervals.

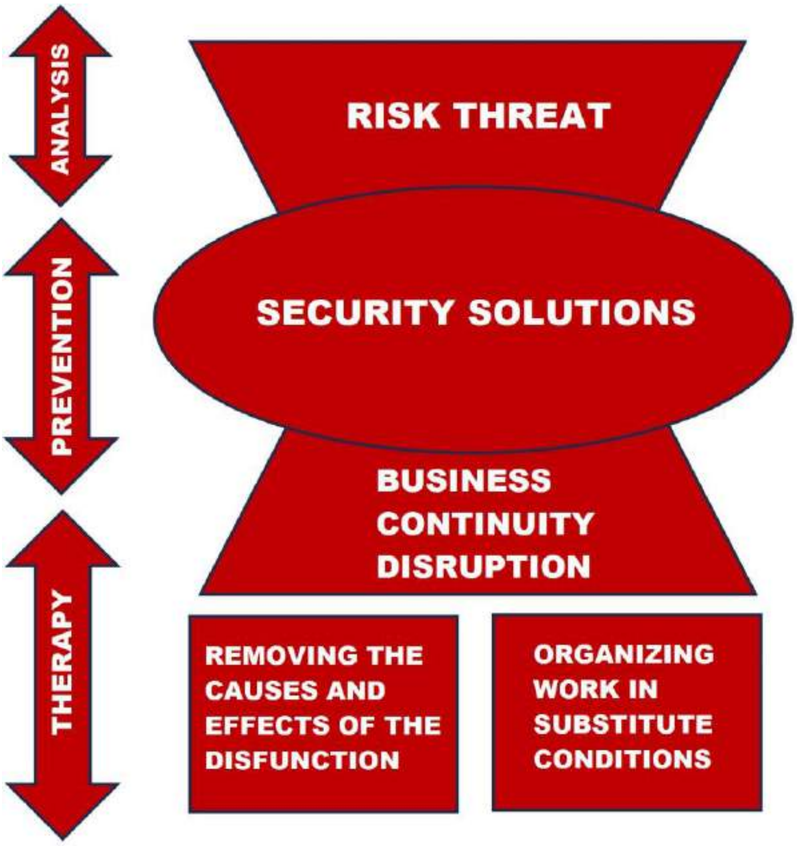
Figure 4. CI protection process in the Deming cycle


•improve by making modifications and corrections
•indicate the scope, goals to be achieved within the CIP and addressees
apply
plan
check
execute
•test and review your CI protection system
• identify critical resources, functions and dependencies, define goals and responsibilities
• perform a risk assessment
• indicate action priorities and prioritize them
• develop and implement a CIP system

Source: National Critical Infrastructure Protection Program – consolidated text, 2023.

All actions taken to ensure CI protection should be proportional to the level of risk of disruption to its functioning. This applies to both the adopted CI protection model, its types, and the forces and means used. From the point of view of the Program, this is a key element that determines and justifies actions taken to reduce the risk of disruption of CI functioning to an acceptable level. Risk assessment should be the basis for defining CI protection standards and setting action priorities. In the context of the Program, risk should be understood as a function of threat, vulnerability and impact. Figure 5 presents the essence and challenges of critical infrastructure security based on the triad: risk - security - continuity.

Figure 5. The concept of connections in the risk triad


ANALYSIS
PREVENTION
THERAPY
RISK THREAT
SECURITY SOLUTIONS
BUSINESS CONTINUITY DISRUPTION
REMOVING THE CAUSES AND EFFECTS OF THE DISFUNCTION
ORGANIZING WORK IN SUBSTITUTE CONDITIONS

Source: Zawiła-Niedźwiecki J., Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji, Wydawnictwo Edu-Libri, 2013 r.

Periodic assessment of the risk of disruption to the functioning of critical infrastructure should be carried out:

- along with the identification of new threats that affect or may affect the proper functioning of critical infrastructure,
- together with the review (update) of the critical infrastructure protection plan,

- to ensure compliance with all government documents.

The CI protection system should apply to all types of identified threats, both natural, intentional and technical, and should be prepared to restore the functions performed by a given CI as quickly as possible. Moreover, it should be comprehensive and flexible and, last but not least, easy to use and understand by those responsible for CI protection.

Actions taken to ensure security are aimed at minimizing the risk of CI disruption by:

- reducing the likelihood of a threat occurring,
- reducing susceptibility,
- minimizing the effects of the threat.

These activities include:

1. ensuring physical security - a set of organizational and technical activities aimed at minimizing the risk of disruption to the functioning of CI as a result of the actions of people who unauthorizedly attempted to enter or found themselves in the CI area;
2. ensuring technical security - a set of organizational and technical activities aimed at minimizing the risk of disruption of CI functioning as a result of disruption of technological processes;
3. ensuring personal security - a set of organizational and technical activities aimed at minimizing the risk of disruption of CI functioning as a result of the actions of persons who have authorized access to critical infrastructure;
4. ensuring ICT security - a set of organizational and technical activities aimed at minimizing the risk of disruption of CI functioning as a result of unauthorized influence on control equipment and ICT systems and networks;
5. ensuring legal security - a set of organizational and technical activities aimed at minimizing the risk of disruption of CI functioning as a result of legal actions of external entities;
6. business continuity and recovery plans, understood as a set of organizational and technical

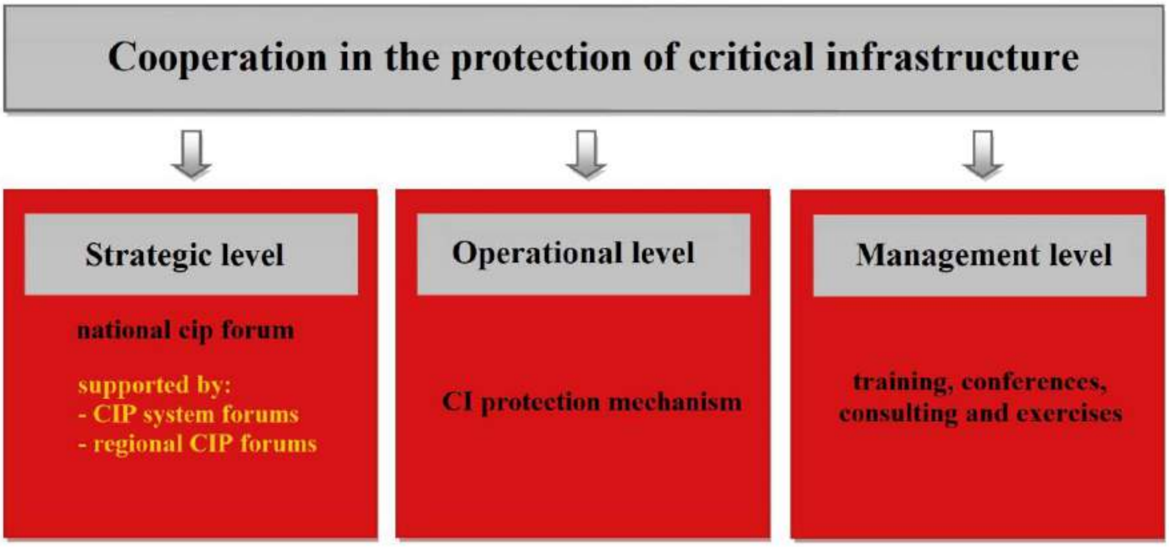
activities leading to the maintenance and recovery of functions performed by CI;

7. the use of specific security measures should be closely related to the assessment of the risk of disruption of CI functioning.

Cooperation, as one of the most important principles of the Program, is a key element ensuring consistency of decisions made and effectiveness of actions implemented both in the course of ongoing work and in situations of threat. To be effective, it should be conducted at the national, systemic, regional and local levels, and involve critical infrastructure operators, regardless of their form of ownership. It also requires the establishment of mechanisms to facilitate it. The conditions for effective cooperation are its authenticity, reciprocity and striving for common benefits.

Cooperation in the CI area means the exchange of all information that may affect the achievement of the Program objectives and maintaining constant contacts between participants of the CI protection process.

Figure 6. Model of cooperation in CI protection



Critical Infrastructure Protection Program – consolidated text, 2023.

Functionally configured exchange of information in the field of critical infrastructure protection will take place in three areas:

1. critical infrastructure protection forum,
2. ongoing exchange of information through direct contacts of the parties (CI protection mechanism),
3. joint training, conferences, consulting and organization of exercises.

The parties to the information exchange discussed will be CI operators and public administration. Experts representing various fields of science and practitioners whose knowledge may constitute added value in the implementation of tasks related to CI protection may be invited to cooperate.

The first area of information exchange in the field of CI protection are **critical infrastructure protection forums**. They will be built to the widest possible extent on the basis of existing forms of coordination and consultation. NPOIK, recognizing the differences between systems and their specificity, does not specify the structure of the forum. The network of system forums reflects a partnership model that will enable the administration and operators of critical infrastructure to undertake a number of activities (e.g. risk assessment, exercises) in a way that takes into account the characteristics of each system. The aim of the forum is to identify key problems in the field of critical infrastructure protection and to initiate work aimed at developing proposed solutions.

Due to the fact that the administration has the opportunity to gather CI protection participants in an environment independent of business conditions, allowing for discussion on the interdependencies of CI systems, cross-system vulnerabilities and issues that are the responsibility of many CI protection participants, it is planned to create CI protection forums at three levels:

- national forum,
- system forums – for each CI system,
- regional (provincial) forums – inter-systemic in nature.

The second area, **the CI protection mechanism, i.e. ongoing exchange of information**, includes the following activities:

1. providing operators with information regarding threats to critical infrastructure,
2. provision by owners and holders of facilities, installations or critical infrastructure devices of information about identified threats to the infrastructure they manage,
3. providing information about the expected or observed increase in demand for services or products provided by operators,
4. functioning of the online platform.

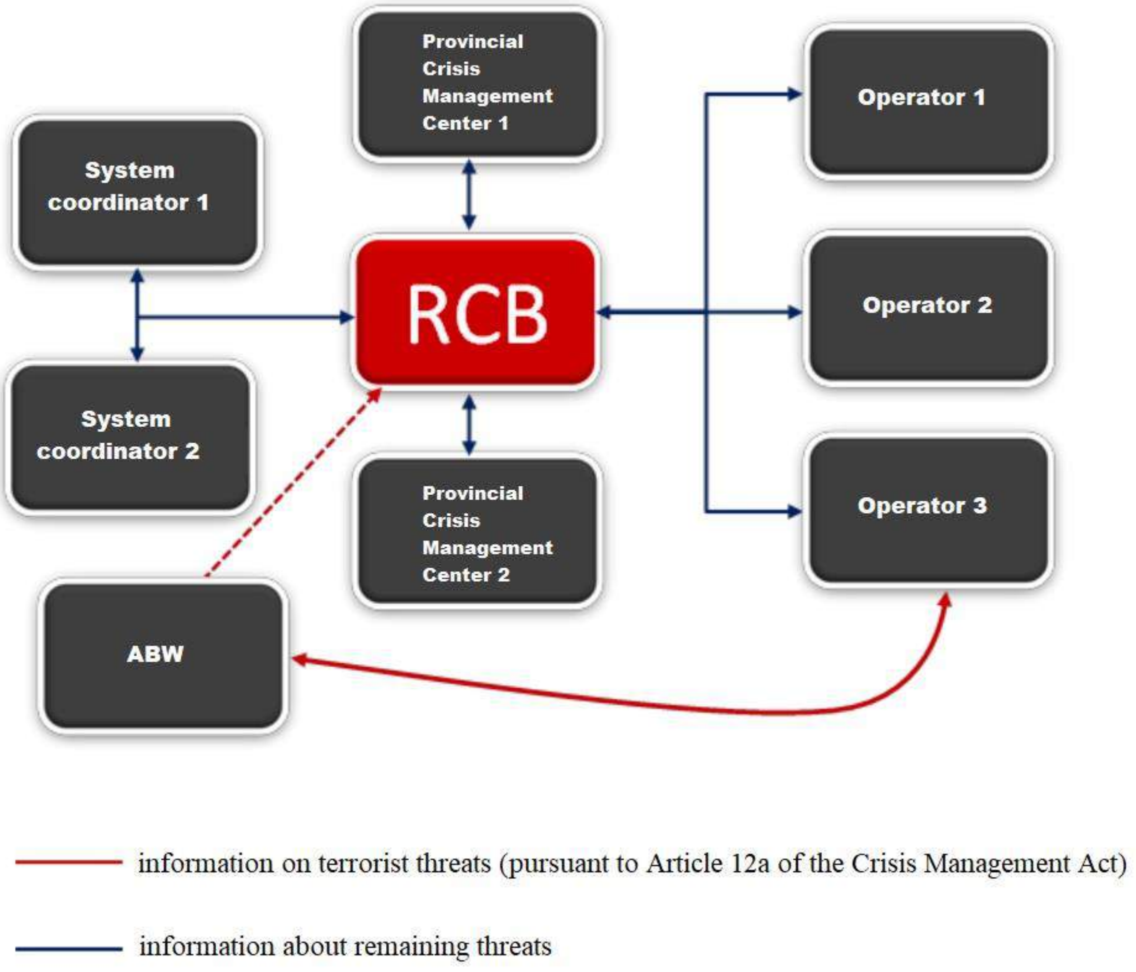
The online platform will act as a platform for exchanging information on threats and vulnerabilities, as well as a platform for developing guidelines for strategies and solutions reducing the risk of disruption of CI functioning, which may later be presented during the meetings of CI protection forums. The platform's members include critical infrastructure operators, representatives of public administration bodies, government agencies, and other involved entities. Its members themselves decide what information is exchanged within the online platform. The exchange of information about threats or identified vulnerabilities may have a positive impact on the image of all entities of the CI system, indicating maturity in the approach to running a business and increasing customer confidence in all entities. The security of information exchanged within the platform is of great importance. The public administration will take all steps to ensure an appropriate level of protection and trust in terms of access by third parties and protection of business secrets.

As part of the mechanism, contact points will be established in public administration units (people responsible for maintaining contacts with entities responsible for the protection of critical infrastructure and CI operators), similarly to CI operators. Contact points are an element of the communication system of institutions related to CI protection.

Up-to-date information on threats to CI facilities and threats to the security of the state and citizens resulting from disruptions in the functioning of CI is crucial for the appropriate response to these threats. Therefore, the RCB is the first point of communication between CI operators, voivodes, CI system coordinators and other entities - this role is performed by the

RCB operational center. Program participants and entities involved in the CI protection mechanism exchange information about threats according to the diagram presented below.

Figure 7. Communication diagram


Provincial Crisis Management Center 1
System coordinator 1
Operator 1
RCB
Operator 2
System coordinator 2
Provincial Crisis Management Center 2
Operator 3
ABW
information on terrorist threats (pursuant to Article 12a of the Crisis Management Act)
information about remaining threats

Source: National Critical Infrastructure Protection Program – consolidated text, 2023.

The third area of ensuring efficient and reliable exchange of information between participants of the CI protection mechanism **are training activities**, necessary to support activities undertaken within CI protection forums. These activities include:

1. providing mutual substantive support (based on consulting and training) by public

administration entities and CI operators,

2. participation of CI operators and administrative entities in exercises in the field of critical infrastructure protection,
3. participation of CI operators and administration entities in conferences on critical infrastructure protection,
4. integration of environments responsible for the protection of critical infrastructure.

Finally, it should be emphasized that the exchange of information as part of the protection of critical infrastructure will be carried out in many ways, through:

- crisis management centers and on-duty services operating 24/7 as part of the crisis management system,
- ongoing, direct contacts between the parties' representatives,
- exchange of open and classified correspondence in a traditional way and using electronic systems for exchanging open and classified information,
- regular, joint meetings as part of critical infrastructure protection forums,
- a common internet platform created specifically for the purpose of exchanging information, presenting experience and knowledge in the field of critical infrastructure protection, cooperation within the forum, organization of meetings, training, etc.

Cooperation within the above-mentioned areas aims to:

- increasing the level of security and reliability of critical infrastructure by: achieving a synergy effect in the activities of CI operators and public administration, effective use of forces and resources allocated to the protection of critical infrastructure and ensuring the exchange of information between CI operators and public administration;
- increasing trust in operators as socially responsible companies by participating in a project aimed at improving the security of systems important for the functioning of society on a national and local level;
- promoting the idea of public-private partnership by: showing the practical advantages of

cooperation between the public and private sectors and identifying and implementing common interests of the public and private sectors.

In the field of critical infrastructure protection, the Government Center for Security (RCB) carries out the tasks specified in Art. 11 section 2 point 11 of the Act on Crisis Management and its implementing acts. Some of these tasks were referred to in Chapters 1 and 4. However, the above-mentioned legal act defines the main tasks of the RCB, which include:[21]

1. civil planning, including: a) presenting detailed methods and means of responding to threats and limiting their effects, b) developing and updating the National Crisis Management Plan, in cooperation with the relevant organizational units of offices serving ministers and heads of central offices, c) analysis and assessment of the possibility of threats occurring or their development, d) collecting information about threats and analyzing the collected materials, e) developing conclusions and proposals for preventing and counteracting threats, f) planning the use of the Armed Forces of the Republic of Poland to perform the tasks referred to in Art. 25 regarding the participation of units of the Polish Armed Forces in the implementation of crisis management tasks, section 3, g) planning support for the implementation of the tasks of the Armed Forces of the Republic of Poland by public administration bodies;
2. monitoring potential threats; 2a) agreeing on crisis management plans prepared by ministers in charge of government administration departments and heads of central offices;
3. preparing to launch procedures related to crisis management in the event of threats;
4. preparing draft opinions and positions of the Team;
5. preparation and technical and organizational support for the Team's work; 5a) ensuring coordination of the information policy of public administration bodies during a crisis situation;
6. cooperation with entities, cells and organizational units of the North Atlantic Treaty

[21] Act of 26 April 2007 on crisis management, as amended, Journal of Laws 2023, item 122, consolidated text

Organization and the European Union and other international organizations responsible for crisis management and protection of critical infrastructure;

7. organizing, conducting and coordinating training and exercises in the field of crisis management and participation in national and international exercises;
8. ensuring the circulation of information between domestic and foreign crisis management authorities and structures;
9. implementation of permanent duty tasks as part of the state's defense readiness;
10. implementation of tasks in the field of preventing, counteracting and removing the effects of terrorist events; 10a) cooperation with the Head of the Internal Security Agency in the field of preventing, counteracting and removing the effects of terrorist events;
11. implementation of planning and program tasks in the field of protection of critical infrastructure and European critical infrastructure, including the development and updating of a functional annex to the National Crisis Management Plan regarding the protection of critical infrastructure, as well as cooperation, as a national contact point, with the institutions of the European Union and the Treaty Organization North Atlantic and their member countries in the protection of critical infrastructure;
12. preparation of the draft order of the Prime Minister referred to in Art. 7, exercising crisis management in the territory of the Republic of Poland, section 4;
13. informing, in accordance with the jurisdiction, the entities referred to in Art. 8 Government Crisis Management Team sec. 2 and 3, about potential threats and actions taken by the competent authorities;
14. cooperation with crisis management centers of public administration bodies.

Special services cooperate with the Government Center for Security in the protection of critical infrastructure, in particular the Internal Security Agency (ABW). This agency is legally obliged to recognize terrorist threats and prevent acts of terrorism. Obtaining and analyzing information allows for the assessment of the sources and scale of the phenomenon, the selection of groups of potential attackers, and identification of their plans and logistical support.

The tasks of the Internal Security Agency also include the recognition, prevention and detection of threats to security, important from the point of view of the continuity of the state's operation of the ICT systems of public administration bodies or the ICT network system included in the critical infrastructure, as well as the ICT systems of owners and possessors of facilities, installations or critical infrastructure devices.

In order to prevent and combat terrorist events relating to ICT systems of public administration bodies or ICT networks covered by a uniform list of facilities, installations, devices and services included in critical infrastructure, which are important from the point of view of the continuity of the functioning of the state, as well as ICT systems of owners, holders autonomous and dependent facilities, installations or critical infrastructure devices or data processed in these systems, as well as the prevention and detection of terrorist crimes in this area and the prosecution of their perpetrators, the Internal Security Agency may assess the security of these IT systems. This assessment is generally carried out in accordance with the annual security assessment plan and involves carrying out security tests of the ICT system in order to identify its vulnerabilities, i.e. weaknesses in the resource or security of the ICT system that may be exploited by a threat affecting the integrity of the IT system, confidentiality, accountability and availability of this system. Moreover, in the event of receiving information about the occurrence of a terrorist event regarding the above-mentioned systems, the Head of ABW may request information on the structure, operation and principles of operation of the IT systems held, including information including computer passwords, access codes and other data enabling access to the system and their use, in order to prevent and respond to terrorist events relating to these systems or data, as well as preventing and detecting terrorist crimes in this area and prosecuting their perpetrators. The head of the Internal Security Agency also keep a register of events violating the security of ICT systems.

Moreover, in order to prevent, counteract and detect crimes of a terrorist nature and to prosecute their perpetrators, the court, at the written request of the Head of the Internal

Security Agency, submitted after obtaining the written consent of the Public Prosecutor General, may, by way of a resolution, order the blocking by the service provider providing services electronically of the availability in the IT system of specified IT data related to a terrorist event or specific IT services serving or used to cause a terrorist event, hereinafter referred to as "availability blocking".

In the event of the introduction of a second or higher alert level, the Head of the Internal Security Agency, in consultation with the minister responsible for internal affairs, may also issue to the Police a recommendation for special protection of individual critical infrastructure facilities in the area covered by the alert level, taking into account the type of threat of a terrorist event.[22]

[22] Ministry of Internal Affairs and Administration, https://www.gov.pl/web/mswia/abw; Act of May 24, 2002 on the Internal Security Agency and the Intelligence Agency, as amended, Journal of Laws 2023, item 1136, consolidated text

6. Natural threats, failures and attacks on Critical Infrastructure, countermeasure options.

Critical infrastructure should be characterized by two very important features, namely integrity and functionality.

Critical infrastructure integrity refers to the condition in which critical infrastructure remains intact and unchanged. This means that it is free from damage, failure, disruption or interference that may interfere with its required operation. Protecting the integrity of critical infrastructure includes both preventive and emergency response measures to minimize the risk of damage. CI functionality means its ability to perform assigned tasks and provide services in an effective and continuous manner. Protecting the functionality of critical infrastructure includes preventing failures, monitoring its condition and performance, and taking quick action in the event of problems to restore normal operation.

One of the key goals of critical infrastructure management is to maintain its integrity and functionality. Achieving this goal includes the planning function, investing in appropriate security measures and responding in the event of failures and/or threats. Threats to maintaining the integrity and functionality of critical infrastructure may result from various reasons, such as cyber attacks, natural disasters, armed conflicts, terrorist attacks, failures or natural wear and tear. Hence, a particularly important task related to maintaining the integrity and functionality of critical infrastructure is adapting the protection strategy to changing environmental conditions and threats, as well as continuous risk assessment.

In the field of safety, it is generally accepted that events can only have adverse consequences, and therefore risk management focuses on preventing and limiting damage. Depending on the size of the impact of the disruption (incident) on the facility/organization and the probability of the disruption occurring[23], there are four basic strategies for responding to threats: the tolerance strategy (T) (external disruptions that are non-invasive and non-destructive, rarely occurring, having a low impact, without lasting damage), strategies monitoring (M) (small

[23] Zawiła-Nadźwiecki J. Metoda TISM-BCP – Total Security Management, Business Continuity Planning, European Network Security Institute, Warszawa 2003.

disruptions, non-destructive, frequent, known with information facilitating the implementation of compensation mechanisms), prevention strategy (Z) (called prevention strategy, used in cases of high probability of disruptions to important elements of activity, in particular sensitive infrastructure elements technical, the degree of destruction of which is unacceptable) and the strategy of continuity plans (P) (significant, destructive disruptions with a very low probability of occurrence). Depending on the nature of the critical infrastructure, due to its role in securing the functioning of the state, it is justified to use strategy (Z) and even business continuity management based on the Continuity Plans Strategy. Business continuity management is defined as "*a holistic management process that aims to determine the potential impact of disruptions on the organization and create conditions for building resilience to these disruptions and the ability to respond effectively to protect key... values achieved in its current operation*".[24]

Protecting critical infrastructure not only means securing the health and life of citizens, but also translates into their trust in the state apparatus, which has a significant impact on society.

The Government Center for Security has expanded the statutory definition of CI to some extent. According to RCB, critical infrastructure is real and cybernetic systems (facilities, devices or installations) necessary for the minimal functioning of the economy and the state. Emphasizing that the definition also applies to cybernetic systems is particularly important nowadays. Most of the threats that face CI facilities result from cyberattacks. With the introduction of the Crisis Management Act, the concept of critical infrastructure protection was also defined. They are described as a set of organizational activities aimed at ensuring the proper functioning of CI or its quick restoration in the event of threats such as failures, attacks or other events that disrupt its operation.

Basically, there are three types of threats to CI, namely the forces of nature, device failures and human actions or omissions. In the case of natural threats, we can talk about floods, strong winds, long-term droughts, earthquakes, sudden icing and intense snowfall, but also epidemics (Covid-19). They cause consequences in the form of threats to the health and life of citizens, potential losses of residential infrastructure, personal property, jobs, etc., as well as

[24] Business Continuity Institute: Business Continuity Management: Good Practice Guidelines 2002

negative effects on the environment in the form of losses in biodiversity, degradation of ecosystems and pollution of the natural environment.

Failures of devices and installations can, of course, have many different causes. However, in many cases they result from mistakes made by people or a coincidence of various circumstances. Failures in infrastructure or disruptions in its functioning may lead to fires, uncontrolled explosions, environmental contamination and threats to public health.

This issue is particularly important in enterprises that are CI operators. In such types of enterprises, sudden interruptions in operation caused by unexpected failures expose them to huge financial losses but also limit their operation in public service delivery systems.

Counteracting critical infrastructure failures should primarily involve:

- Monitoring and maintaining the appropriate level of operational efficiency of the existing technical infrastructure through regular inspection, maintenance and modernization to avoid failures caused by wear, aging of equipment or technical errors.
- Emergency response planning: Organizations responsible for critical infrastructure should have emergency response plans in place that include procedures, training and exercises to respond quickly and effectively to emergencies.
- Providing redundancy by securing alternative sources of supply and backup systems that can be activated in the event of a failure.
- Risk management by identifying potential sources of failures and preparing for their effects, thus detecting and eliminating threats before they occur.

The third category of threats are human activities, specifically terrorism, which is an increasingly common threat in modern times. Generally, any facility classified as critical infrastructure can be the target of an attack. First of all, energy supply systems, energy raw materials and fuels, as well as communication systems and ICT networks, financial systems and water supply systems may be exposed to this type of attacks. Health and food supply systems cannot be completely safe from this type of attacks. Nowadays, energy and communication systems are the most vulnerable point, hence the clear change in the target of a possible attack. Acts of sabotage may not only lead to material losses, but also present the Republic of Poland in an unfavorable light in the international arena.

CI is an attractive target of direct terrorist attacks due to the assumed psychological, social, economic and political effect - disruption of the functioning, damage or destruction of facilities or systems that are key to the efficient operation of the entire state. Therefore, building resilience and critical infrastructure protection (CIP) are today one of the greatest challenges for the security of the state and its citizens.[25] Ensuring security resulting from attacks on CI and state citizens includes a set of activities and protective and preventive measures aimed at reducing the sensitivity and susceptibility of certain entities to external attacks, including terrorist ones. Protective tasks are carried out mainly through physical security measures (personal and technical), analysis of information about threats, conducting operational and reconnaissance activities and raising public awareness of the response.

The basis of any system of protection against attacks, including terrorist CI attacks, of the country, persons or devices, are legal provisions and mechanisms for their continuous updating. At a minimum, the system should keep up with permanent changes in the sources and nature of threats.To ensure effective protection, it is important to implement new methods and measures aimed at identifying potential threats, reducing their impact and identifying the vulnerability of individual system elements. Risk assessment and standardization of threat analysis are of particular importance in this context. Popular methods used, e.g. for physical objects, are CARVER, CARVER+Shock, SVA, threat matrix[26]. It is important to identify various types of terrorist projects to recognize the possibility of terrorists operating in a specific structure in a given geographical area. These possibilities can be reduced to four pillars[27]:

a) **direct target of the attack** – selected precisely due to its distinctive features, e.g. access to the facility, type of security, etc.,

[25] Infrastruktura krytyczna – Rządowe Centrum Bezpieczeństwa (rcb.gov.pl) (01.09.2023)

[26] M. Kupniewski, *Metody i kryteria oceny stopnia zagrożenia atakiem terrorystycznym*, „Przegląd Policyjny" 2018, nr 4 (132), s. 94-107.

[27] R.V.G. Clarke, G.R. Newman, *Outsmarting Terrorist*, Praeger Security International, Westport-London: 2006 s. 9.

b) **type of weapon** - access to a specific category of weapon and the ability to use it,
c) **tools** – cars, financial resources (money transfers, credit cards, cash), mobile phones, etc.,
d) **favorable conditions** - e.g. lack of border controls, leaky banking system, etc.,

A terrorist attack usually occurs where favorable circumstances exist. It is related to the ability to penetrate the social environment and reach new technologies in order to take over the physical systems, resources and services that support this society in its everyday functioning.

The risk assessment of terrorist threats to areas, facilities and devices subject to protection is created based on the catalog of incidents contained in the Regulation of the Minister of Internal Affairs and Administration of July 22, 2016 (Journal of Laws of 2016, item 1092). Estimating the level of terrorist threat to the protected facility, area and device should also take into account the knowledge management system in critical infrastructure elements.

Resilience is not a fixed element of the system. The ability to respond in real time to the changing nature of threats assumes a flexible approach to risk assessment. CI protection in Poland generally focuses on critical gaps, the so-called vulnerabilities, and less on the necessary requirements, i.e. basic conditions that strengthen resilience, means and resources, including human resources.

European Union structures participate in developing standards and good practices in the field of CI protection against terrorism. In December 2020, the European Commission presented a new **Anti-Terrorism Agenda**. The Counter-Terrorism Program aims to support Member States to better anticipate, prevent, protect and respond to the terrorist threat. The priorities include building resistance to terrorist attacks of critical infrastructure, including improving the level of cybersecurity.

7. Legal, physical, personnel, technical and ICT security of Critical Infrastructure.

As mentioned in previous chapters, security measures are aimed at minimizing the risk of disruption to critical infrastructure by reducing the likelihood of a threat, reducing vulnerability to a threat, and minimizing the consequences of a threat. The National Critical Infrastructure Protection Program assumes that these measures will be taken in such areas as:

1. ensuring physical security;
2. ensuring technical security;
3. ensuring personal security;
4. ensuring ICT security;
5. ensuring legal security.

Ensuring physical security is a set of procedural, organizational and technical measures aimed at minimizing the risk of disrupting CI operations as a result of the actions of individuals who have unauthorizedly attempted to enter or have entered CI. It consists of, among other things, direct physical protection and technical (electronic and mechanical) safeguards.

Direct physical protection and technical security achieves its objectives through, among other things:

- prevention,
- detection,
- transmission of information about the detection of an intruder (alarming),
- delaying the intruder from reaching protected areas,
- response/intervention for an incident.

In addition to the aforementioned functions, the physical security system can perform the functions of deterring an attacker, such as at the prevention stage (e.g., message boards), alarming (outdoor sirens) and intervention (calling for lawful behavior). The evidentiary function is also partially realized in the case of video surveillance systems. It should be noted that no physical security measures will provide total security. Protective measures only increase the likelihood of effective counteraction.

Ensuring technical safety is a set of organizational and technical measures aimed at minimizing the risk of disruption to the operation of facilities, installations, technical or water equipment and services to ensure the continuity of their operation.

The basic and most effective way to ensure technical safety of CI is to comply with the legal acts, standards, operating regimes applicable to the infrastructure in question, as well as to implement expert recommendations and findings resulting from the risk assessment adopted and implemented by the CI system coordinator or CI operator.

The purpose of technical safety is to maintain the safe functionality of the relationship between employees and management and technology, including facilities, installations, equipment and maintenance services - the environment, and to maintain the balance of this relationship with the environment and climate.

Ensuring personal security is a set of measures and procedures aimed at minimizing the risk associated with persons who, through authorized access to facilities, devices, installations and services of critical infrastructure, may cause disruptions in its operation.

Staff members associated with critical infrastructure facilities, devices, installations and services, as well as persons temporarily staying within CI (service providers, suppliers, guests) may pose a potential threat to its functioning. The position occupied in the CI operator's structure determines the level of physical access to subsequent security zones and access to sensitive, not necessarily classified, information. Both of these privileges may be used illegally and serve to disrupt the functioning of CI or act to its detriment (this also applies to service providers, suppliers and guests).

More than 85% of fraud in companies is caused by people from inside the company. It should be remembered that many aspects of ensuring personal security are inextricably linked to other elements of the CI security system, such as ensuring physical or ICT security. Only the complementarity of all elements will ensure a satisfactory level of CI security against internal threats, e.g. disappointed employees, provocations, competition or organized crime.

The basis for the effectiveness of ensuring personal security is collecting as much information as possible, obtainable under applicable law, about a potential employee during the recruitment process. In order to optimize the time, effort and resources used in the recruitment procedure, first of all, a candidate's profile should be carefully prepared, and a precise definition of the scope of responsibilities will determine the level of access to zones, rooms, depositories, etc. that will be granted to him and what sensitive information he will have at his disposal.

The priority in ensuring personal safety is to thoroughly check the employee (e.g. analysis of submitted documents and verification of their authenticity) before employing him, but safety rules for those already employed in the organization must not be neglected. During employment, in the event of a change of job position, the rights granted to the person should be verified and adapted to the currently held position. All rights that the employee had in connection with the previously held position should be withdrawn. In this case, information from the HR department about the change of position to other organizational units, including those responsible for security, is of key importance. It is also advisable to periodically verify the necessity of authorizations granted to all persons - employees and external subcontractors.

Ensuring the ICT security of critical infrastructure is a set of organizational and technical activities aimed at minimizing the risk of disruption of CI functioning as a result of unauthorized influence on control equipment and ICT systems and networks, including acts of broadly understood cybercrime and cyberterrorism as well as accidental (unintentional) actions of users.

Nowadays, an effective cyber attack on CI may directly affect the security of the state and its citizens. Critical infrastructure is exposed to cyberattacks carried out by both beginners and highly specialized cybercriminals, who may disrupt its functioning and the effects of random events such as system failures, malfunctions of devices or programs supporting it.

Ensuring legal security is a set of activities aimed at minimizing the risk associated with the activities of natural persons or other economic entities (state or private), whose activities may lead to disruptions in the functioning of CI facilities, devices, installations and services.

When ensuring legal security, we primarily mean the tools used by the state to secure the most important CI facilities against threats. This means the use of legal tools that prevent, through the possibility of controlling and possibly blocking or limiting management decisions, e.g. a hostile takeover, merger or sale of certain infrastructure elements, which may result in disruptions in its functioning.

Such tools are provided by the Act of March 18, 2010 on special powers of the minister responsible for state assets and their exercise in certain capital companies or capital groups operating in the electricity, crude oil and gas fuels sectors (Journal of Laws of 2020, item 2173).

Ensuring legal security within the meaning of the Act on Special Powers... applies only to entities whose property has been included in the uniform CI list in the energy, energy raw materials and fuel supply system.

Regardless of the solutions adopted by the state, all legal actions should be taken to minimize the risk of disruption to the functioning of CI. Securing the legal title to the real estate where CI is located, allowing for the enforcement of access to CI, and securing contracts with media suppliers are examples of good practices in this area.

It should be remembered that **actions taken to ensure physical, technical, personal,**

ICT and legal security are preventive actions that are intended to prevent the risk of a crisis from materializing. Despite proper implementation of security programs, it is not possible to 100% eliminate the risks related to interruption of business processes. Therefore, business continuity plan(s) must be developed and implemented.

After responding to the incident and ensuring the continuity of key processes, full (normal) functionality of the critical infrastructure should be restored as soon as possible. To do this in an efficient and cost-effective manner, appropriate recovery plans must be prepared in advance (these plans may be part of the business continuity plan).

The effects of threats should be assessed at the risk assessment stage. Although it is impossible to predict all incidents and their interactions, plans should be as concise as possible. In small organizations, a single plan covering all activities needed to restore full functionality of the critical infrastructure is enough. In large organizations, it is reasonable to divide the plan into parts, each of which presents in detail how to return to normal operation of facilities, services, devices and installations as a result of various types of incidents. Each plan should include the following elements:

- Intent and scope;
- Goals;
- Launch criteria and procedures;
- Implementation procedures;
- Roles, responsibilities and authorities;
- Communication requirements and procedures;
- Internal and external connections and impacts;
- Resource requirements;
- Information flow and documentation processes.

Both business continuity and reconstruction plans as well as personal, legal,

physical, ICT and technical protection must be treated equally as key elements of security management. Safety management also requires interdisciplinary organizational, engineering and humanistic knowledge as well as focus on managerial and employee competences in all its most important processes and services supporting them. Having knowledge about threats, their areas of occurrence, mutual connections and interdependencies, as well as the ability to take preventive actions and in the processes of materializing threats allows all employees and stakeholders to build security responsibly and permanently.

8. European critical infrastructure - new system solutions and protection technologies.

European critical infrastructure is defined in Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure, as well as the Act of 26 April 2007 on crisis management implementing its provisions. According to the directive, **critical infrastructure** is "a component, system or part of infrastructure located in the territory of the Member States which is essential for maintaining essential social functions, health, safety, security, material or social well-being of the population and whose disruption or destruction would have a significant impact on the Member State concerned as a result of the loss of these functions” (Article 2(a)). **European critical infrastructure** is defined as "critical infrastructure located in the territory of the Member States, the disruption or destruction of which would have a significant impact on at least two Member States; whether the impact is material is assessed against cross-cutting criteria; this includes effects arising from cross-sectoral interdependencies with other types of infrastructure” (Article 2(b)).

Therefore, the following properties of critical infrastructure elements are distinguished:

- constitute a fragment, part, component or entire infrastructure system in a given State,
- enable the performance or delivery of primarily social, health or safety functions,
- cause a negative impact on the immediate or distant environment in the event of

dysfunction.

The determination of the materiality of the impact shall be assessed in relation to cross-cutting criteria defined on a case-by-case basis by the Member States concerned by the critical infrastructure concerned. The Polish Act on Crisis Management of April 26, 2007, taking into account the principles of designating European critical infrastructure and the sectors from which it may be designated, provides in Art. 3 point 2a, the following definition of European critical infrastructure: "systems and functionally interconnected objects included in them, including buildings, devices and installations that are key to the security of the state and its citizens and serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs , designated in the systems: energy supply system, energy raw materials and fuels and transport system, in the field of electricity, crude oil and natural gas and road, rail, air, inland waterway transport, ocean shipping, short sea shipping and ports, located in the territory of the Member States of the European Union, the disruption or destruction of which would have a significant impact on at least two Member States.

The designation of European critical infrastructure was guided by the idea of improving the process of protecting citizens, which constitutes an important part of the activities undertaken under the European Critical Infrastructure Protection Program, which consists primarily of:

- CIPS program[28] – „Prevention, preparedness and management of the effects of terrorism and other types of security risks",
- Critical Infrastructure Warning Information Network (CIWIN) enabling the transmission of warnings and exchange of experiences within an electronic forum,
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the needs for improving its protection of 2008,
- helping Member States work on national solutions in the field of critical infrastructure,

[28] Terrorism & other Security-related Risks (CIPS), https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks_en (dostęp: 07.09.2018 r.)

- cooperation with third countries,
- contingency plans[29].

The basic principles established in the European Critical Infrastructure Protection Program are:

The principle of subsidiarity - specifying that the primary and final responsibility for the protection of critical infrastructure lies with the Member States and the owners and operators of critical infrastructure, and assistance in the event of support provided by other Member States and the European Commission is provided only in the case of infrastructure that may cause cross-border consequences,

The principle of complementarity - recognizing in the Community approach the experiences, requirements, measures and specificities already applied by individual sectors at Community, national and regional level, including those relating to mutual assistance agreements

The principle of confidentiality - determining the coherence and effectiveness of the exchange of information on critical infrastructure in relations between Member States and between Member States and the European Commission,

The principle of cooperation between interested parties - enabling the adoption of common guidelines on actions and instruments for the protection of critical infrastructure,

The principle of proportionality - including the strategies and measures used to the level of potential risks

The principle of recognizing differences between sectors - recognizing that the characteristics of individual sectors, despite some common elements, are in principle unique and require an individual approach[30].

To sum up, it should be emphasized that the protection of critical infrastructure in the European Union Member States is carried out according to defined protection frameworks, which include, among others:

- common rules for the protection of critical infrastructure,

[29] R. Wróbel, Przygotowanie podmiotów infrastruktury krytycznej, Warszawa 2016
[30] Ibid.

- common definitions,
- jointly defined scope of responsibilities of entities,
- common list of European critical infrastructure sectors,
- common procedure for infrastructure protection plans for European critical infrastructure,
- common procedure for the recognition by Member States of critical infrastructure that may be designated as European critical infrastructure,
- common methods for identifying and classifying the risks, threats and vulnerabilities associated with individual infrastructure components to improve the protection of European critical infrastructure.

Cooperation between Member States in the area of critical infrastructure protection is based on bilateral or multilateral agreements, and often begins when the value of cross-cutting criteria is established in relation to critical infrastructures that may be designated as European critical infrastructure. Nevertheless, the owners and operators of European critical infrastructure, alongside the Member States, are fundamentally and ultimately responsible for the protection of critical infrastructure. In order to ensure a Community approach to the protection of critical infrastructure, Member States may, where appropriate, conclude mutual assistance arrangements of a cross-border nature[31].

At the end of 2020, the EC proposed two directives promoting a systemic approach to CI protection and counteracting modern threats. These directives are part of a package of legislative measures aimed at increasing the resilience and capacity of public and private entities in the EU to respond to cybersecurity incidents and protect critical infrastructure.

The first one concerned **improving the critical entities resilience** (CER Directive) extending the European Critical Infrastructure (ECI) Directive of 2008.[32] The second one is a response to growing cyber threats and concerns measures **for a high common level of cybersecurity**

[31] R. Wróbel, Przygotowanie podmiotów infrastruktury krytycznej, Warszawa 2016.

[32] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=LEGISSUM:4632724 (12.09.2023)

throughout the Union (NIS2 directive - entered into force in 2023).[33] **The directive introduces changes**, among others: two types of entities: essential entities and important entities, expands the subjective scope of the NIS Directive to include public administration, food sector, sewage, industry, waste management and space, increases requirements in the field of cybersecurity.

In the years 2023-2024, there have been (and are still taking place) fundamental changes in CI protection in EU countries, due to the need to implement the CER Directive. These changes mean, among others: standardization of protection of CI facilities, criminal and financial sanctions for CI operators for maintaining the "illusion of security". The draft CER directive moves away from the current approach to CI protection, which is based on the protection of a limited number of physical infrastructure elements, in favor of increasing the resilience of those critical entities that provide services important from the perspective of a properly functioning internal market. The consequence of the entry into force of the provisions of the CER Directive will be a significant expansion of the scope of private entrepreneurs who will be identified as critical entities. The directive does not differentiate obligations depending on the nature of the entity. The same requirements will apply to both public entities or companies with State Treasury participation, as well as to private entrepreneurs. The introduction of new, important obligations for entrepreneurs will require equipping them with, among others: with appropriate legal tools enabling these entities to perform them.

In order to invest in the resilience of CI, the European Commission intends to establish expert missions to support Member States in carrying out risk assessments and to strengthen the resilience of European cities as the main attractors (direct targets) of terrorist attacks. In addition, the EU has planned activities to disseminate knowledge and experience in preventing radicalization of attitudes and behavior, an important element of anti-terrorism policy, through, among others, creation of an **EU Knowledge Hub** and implementation of financial support instruments from the Internal Security Fund.[34]

[33] https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive (12.09.2023)

[34] Security Union: A Counter-Terrorism Agenda and stronger Europol to boost the EU's resilience Brussels, 9 December 2020, online: A Counter-Terrorism Agenda (europa.eu); (12.09.2023 r.)

These new activities clearly define the directions of critical infrastructure protection, also in Poland. In the coming years, a dynamic increase in the number of facilities with CI status and growing needs to build their resilience should be expected. Multi-level cooperation and real involvement of public administration, business, academia and anti-terrorist education of citizens will become the key to systemic and effective protection of goods and services provided to citizens.

As repeatedly indicated above, the protection of critical infrastructure is a key task ensuring national security and stability in the provision of public services. Given the widely observed technological progress, new technologies play an increasingly important role in improving the efficiency and effectiveness of critical infrastructure protection. Here are some new technologies that are increasingly being used to protect critical infrastructure:

- **VMS systems** enable the operation of a large number of cameras and the recording of images generated by them, as well as integration with other network electronic security systems. Such comprehensive security systems can both protect critical infrastructure facilities against access by unauthorized persons and supervise operational processes, optimize production efficiency, monitor employee safety and assess the risk of possible accidents in real time and prevent them.

- **Augmented Reality (AR) and Virtual Reality (VR)**. AR and VR technologies are used to train personnel responsible for protecting critical infrastructure. They can provide realistic simulations of emergency situations, enabling staff to be better prepared to operate in difficult conditions.

- **Database analysis (Big Data):** Large amounts of data generated by various monitoring systems and sensors can be analyzed using advanced data analysis tools. This allows you to detect patterns and anomalies that may indicate potential threats.

- **Artificial intelligence (AI) and machine learning.** AI algorithms and machine learning are used to automatically detect threats, analyze unsafe behavior and prevent incidents in real time.

- **Neural networks and deep learning.** These technologies are used to recognize patterns in images and sounds, which can help identify unwanted events such as attacks or crashes.

- **Internet of Things (IoT):** IoT sensors and devices can be used to monitor the health of critical infrastructure in real time. Thanks to them, you can collect data on temperature, humidity, vibration, pressure, etc., which allows you to quickly respond to possible problems.

- **Blockchain.** Blockchain technology can be used to secure data related to critical infrastructure, preventing forgery and unauthorized access to data.

- **Cybersecurity solutions.** Modern cybersecurity solutions such as behavior recognition, firewalls and encryption algorithms.

- **Drones.** Drones can be used to inspect and monitor critical infrastructure, especially in hard-to-reach places. They can also help with emergency management and providing disaster relief.

- **5G technology.** Fast and reliable 5G connections can be used to remotely monitor and control critical infrastructure systems in real time.

- **Renewable energy and microgrids:** The use of renewable energy sources such as solar and wind, combined with microgrids, can increase the resilience of critical infrastructure to energy supply failures.

New technologies in the protection of critical infrastructure are necessary to effectively manage and minimize the risk associated with potential threats. However, it is equally important that appropriate procedures, regulations and training are adapted to these new technologies to ensure comprehensive protection of critical infrastructure.

List of shortcuts

ABW – the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego)

CI – critical infrastructure

NPOIK – the National Critical Infrastructure Protection Program (Narodowy Program Ochrony Infrastruktury Krytycznej)

CIP – critical infrastructure protection (CIP)

RCB – the Government Security Center (Rządowe Centrum Bezpieczeństwa)

RP – The Republic of Poland

CIS – Critical infrastructure systems

UZK – the Law on Crisis Management (Ustawa o zarządzaniu kryzysowym)