PROTECTION OF NATIONAL AND EUROPEAN CRITICAL INFRASTRUCTURE

Tadeusz SZCZUREK

Military University of Technology

Marzena SZCZUREK

Central Contamination Analysis Centre in Warsaw

Abstract. Protection of national and European critical infrastructure in the territory of the Republic of Poland is a complex process requiring the efforts of a number of public and private institutions. In particular, owners and users of critical infrastructure systems are obliged to provide such protection. These are key responsibilities from the point of view of national security, as destruction, damage, failure or any other deprivation of the functioning of critical infrastructure could pose a serious threat to the functioning of society on a local, national or even European scale. Indeed, a number of systems cover more than one country. Even if an infrastructure is located in a Member State of the European Union, but its disruption or destruction would have a significant impact on at least two Member States, it is classified as 'European Union critical infrastructure'. In Poland, critical infrastructure comprises eleven systems comprising facilities, equipment, installations, and services crucial for the security of the state and its citizens. The operators of this infrastructure are both state entities and private owners, however, competent ministers and heads of central offices are responsible for individual systems at the national level. The National Program for Critical Infrastructure Protection is an important document regulating the issues of critical infrastructure protection in Poland. The main objective of the program was to create the conditions for enhancing the security of critical infrastructures, covering all four phases of crisis management: prevention of disruption, emergency preparedness, emergency response and restoration of damaged critical infrastructures. According to the Crisis Management Act, the Director of the Government Security Center is the person responsible for the coordination of all projects and the main executor of the draft program. Detailed information on critical infrastructure is prepared by the Ministers responsible for these systems. The program comes into force after approval of its draft by the Council of Ministers. All levels of public administration are involved in the implementation of tasks included in the National Program for Critical Infrastructure Protection. This is primarily related to the duties of the government and local government administration in the area (sphere) of crisis management. The first program in Poland was introduced on 30 April 2010 by a relevant regulation of the Council of Ministers. The program is updated at least every two years. The 2015 version is available on the website of the Government Security Center[1]. The next version of this document will be available soon.

Keywords: security, national security, regional security, infrastructure, critical infrastructure, National Program for Critical Infrastructure.

[1] http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf [Access on 10.03.2018].

Introduction

Protection of critical infrastructure is a process of fundamental importance for the functioning of the state and its security in structural and personnel terms. In Poland, this process was intensified by the adoption of the Crisis Management Act and, in particular, its amendment in 2009, when entities responsible for ensuring the continuity of operation of eleven systems constituting critical infrastructure were very clearly identified.

The formal and legal definition of critical infrastructure included in the Act on crisis management refers to systems containing facilities, devices and services crucial for the security of the state and its citizens. In particular, critical infrastructure includes: 1. energy, energy resources and fuel supply systems; 2. communications systems; 3. information and communication networks systems; 4. financial systems; 5. food supply systems; 6. water supply systems; 7. health protection systems; 8. transport systems; 9. emergency systems; 10. systems providing continuity of public administration; 11. systems for production, warehousing and storage of chemical and radioactive substances, including pipelines of hazardous substances[2].

Each of these systems contains elements that are particularly sensitive to external and internal threats. It is therefore necessary to define these threats and to identify the facilities to be protected as critical infrastructure elements. Such an indication is important because not all – even apparently crucial and important – facilities or systems are classified as critical infrastructure. The experts in crisis management, on whom the main burden of separating critical infrastructure elements from the surrounding reality has fallen, must focus not so much on facilities or devices as on services and functions that infrastructure performs in relation to the society, and in particular take into account the vulnerability of society to disruptions in the functioning of the systems in question[3].

Substantive discussion in search of the best solutions in the area of Critical Infrastructure Protection has been going on for many years in the most important scientific centres dealing with national security. For example, the First International Scientific Conference on "Critical Infrastructure Protection – Diagnosis of Needs and Opportunities" took place at the Police Academy in Szczytno on 15-16 March 2010. It was an important stage in the implementation of the research project under the name: "Participation of the Police in Critical Infrastructure Protection in ensuring security and law and order". Recently, the Szczytno Academy organized

[2] Act of 28 April 2007 on crisis management, Journal of Laws of 2007, No. 89, item 590, as amended, Article 3.2.

[3] Skomra, *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, [in:] A. Tyburska (ed.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010, p. 211.

a conference on "Participation of the Police and other services and institutions in the protection of the state's critical infrastructure in the era of asymmetrical threats – diagnosis and perspectives". The conference was held on 27-28 February 2018 and its subject confirms the process of evolution of the increasingly interdisciplinary approach to security, including the protection of critical infrastructure, in the Polish science. The participants of the latter conference stressed the service role of critical infrastructure and the need to focus efforts on securing its continuity. Such a look at critical infrastructure confirms the validity of the directions adopted a few years ago for changes in the organization of the protection of such infrastructure. Dynamic changes in the security environment, including the emergence of new threats, must be taken into account.

1. Critical infrastructure protection in national and international security systems

Among the national security infrastructure[4], or more broadly among the key state infrastructure[5], the critical infrastructure is situated as one without which it is impossible to speak of ensuring the security of individual and collective entities forming a nation[6] and a state. Critical infrastructure is the basis for the functioning of a state and nation, inscribing itself in the essence of its security, which is the certainty of the existence and development of the state and individual members of society forming the state.

On an international scale, the famous energy blackout[7] on the North American continent on 14 August 2003 was a spectacular event which highlighted the need

[4] National security infrastructure includes: 1) critical infrastructure, 2) facilities of particular importance for state security and defense, 3) facilities, areas, equipment and transports subject to mandatory protection (A. Tyburska, *Ochrona infrastruktury krytycznej w Polsce – wyzwania w tworzeniu bezpieczeństwa narodowego*, Academy of National Defense, Warsaw 2013, p. 149).

[5] Key infrastructure of the state includes: 1) critical infrastructure, 2) "government" infrastructure, 3) facilities of particular importance for state security and defense, 4) facilities, areas, equipment and transports subject to mandatory protection, 5) military infrastructure (R. Radziejewski, *Jak ocenić (zmierzyć) bezpieczeństwo kluczowej infrastruktury państwa?*, [in:] M. Cieślarczyk, A. Filipek, A. Świderski, J. Ważniewska (ed.), *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, Volume 1, University of Life Sciences and Humanities, Siedlce 2013, p. 276).

[6] A nation is understood here as a society forming the population of a given country. It should be borne in mind that there are other approaches to the issue of the "nation". For example, a nation can be understood as a homogeneous ethnic group (More: W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Akademia Obrony Narodowej, Warsaw 2011, pp. 16-17).

[7] Blackout is the common name for an interruption in the power system resulting in a loss of voltage in the grid over a large area. Witold Skomra defines "blackout" as "a widespread failure of a power supply system or its parts together with the social and economic consequences of a power failure" (W. Skomra, *Ochrona infrastruktury krytycznej…*, op. cit., p. 210).

to address critical infrastructure protection in a systemic manner. At that time, on the border of the USA and Canada, large fluctuations in energy levels occurred in the power system, which resulted in the automatic shutdown of dozens of power plants. For more than 20 hours, over 50 million people have been disconnected from their electricity supply, inhabiting among others: New York, Detroit, Toronto and Ottawa. The failure forced the closure of all airports in the region. Trains stopped on the routes, elevators stopped in buildings and traffic chaos arose due to the lack of traffic lights. The so-called cascading effect occurred then, characterized by the fact that the destruction or failure of one CI system resulted in the discontinuation or limitation of the operation of other infrastructures. That same year Finland (23 August 2003), England (28 August 2003) and the Czech Republic (2 October 2003) faced blackouts, although on a much smaller scale. The largest power system failure in Europe so far took place on 28 September 2003, when almost all Italy, France and Switzerland were deprived of electricity[8]. Poland was not unaffected by such events either. These were usually the consequences of extreme meteorological events, such as a powerful tornado, which passed over parts of the Opolskie, Śląskie and Łódzkie Provinces on 15 August 2008. In the Częstochowa region alone, 20 thousand people were left without electricity[9]. One of the biggest energy failures in the post-war history of Poland took place on 8 April 2008 in Szczecin. The failure of the power grid caused 70% of the city's inhabitants to be without electricity. There were serious disturbances in the functioning of the water supply and sewage system. School classes were canceled, most of the shops closed, and there were no banks in operation. The city was stuck in traffic chaos. The threat of crime has increased considerably[10].

The creation of a critical infrastructure protection mechanism was recognized by the authors of the National Security Strategy, who saw such a solution as a response to the growing level of threats to infrastructure facilities and systems of key importance for the security of the state and its citizens. Already in 2007, the authors of the strategy wrote: "The development of a national plan for the protection of critical infrastructure and the involvement of operators and infrastructure owners, including private ones, in the construction of the mechanism, in addition to the administration and public service, should be pursued. Being aware of the supranational dimension of the functioning of critical infrastructure, it is necessary to ensure Poland's active participation in the works on its protection carried out on the forum of NATO and the EU"[11]. The provisions of the *Act on crisis management*, which has already been

[8] W. Skomra, *Ochrona infrastruktury krytycznej…*, op. cit., p. 210.

[9] T. Szczurek, *Od deskrypcji do antycypacji wykorzystania potencjału militarnego w kształtowaniu bezpieczeństwa nowoczesnych wspólnot państwowych wobec rozwoju zagrożeń niemilitarnych*, Wydawnictwo Wojskowej Akademii Technicznej, Warsaw 2012, pp. 127-128.

[10] W. Skomra, *Ochrona infrastruktury krytycznej…*, op. cit., p. 210.

[11] *National Security Strategy of the Republic of Poland*, Warsaw 2007, pp. 28-29.

mentioned, correspond with this guiding idea, as it provided legal basis for the issuing of a regulation by the Council of Ministers on the *National Program for Critical Infrastructure Protection*[12].

The provisions of the *Act on Crisis Management* obliged the Director of the Government Security Center – in cooperation with the ministers and heads of central offices responsible for the CI systems and competent for national security issues – to define detailed criteria for identifying the facilities, installations, devices and services included in these systems. As a basic criterion in this respect, the legislator indicated the importance of these elements for the functioning of the state and meeting the needs of its citizens[13]. An important step in the practical implementation of this task was the development by the Government Security Center of detailed criteria allowing for the identification of facilities, installations, equipment and services that are part of the critical infrastructure systems. They were divided into two groups: 1) sectoral (systemic) criteria – characterizing quantitatively or substantively the parameters (functions) of a facility, equipment, installation or service, the fulfillment of which may give rise to classification as a critical infrastructure; these criteria are presented for each of the systems of critical infrastructure; 2) cross-sectional criteria – relating to the effects of destruction or cessation of functioning of a facility, equipment, installation or service identified by means of meeting the sectoral (systemic) criteria[14].

In accordance with the adopted methodology, three stages of selecting critical infrastructure from the social reality were distinguished. In a first step, facilities, installations, devices or services that could potentially be considered critical are pre-selected. At this stage, system specific sectoral criteria are applied. The second stage is to confront the systems selected in the first stage with the definition of critical infrastructure adopted in the *Act on crisis management.* The last stage, the third stage, is the application of cross-sectional criteria, i.e. indicating the effects of the destruction of the selected infrastructure on the security of the state and its citizens[15].

The National Program for Critical Infrastructure Protection is a document presenting the government's vision of protecting the state's infrastructure assets which are key to its functioning. The Program indicates criteria for the identification of critical infrastructure, in particular facilities, installations, equipment and services that are essential for the functioning of the state and for meeting the needs of its citizens. It sets out basic objectives, priorities, requirements and standards to ensure

[12] Regulation of the Council of Ministers of 30 April 2010 *on the National Program for Critical Infrastructure Protection,* Journal of Laws of 2010 No. 83, item 541.

[13] Act of 28 April 2007 *on crisis management...*, op. cit., art. 5b.

[14] M. Pyznar, *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa*, [in:] A. Tyburska (ed.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010, p. 105.

[15] Ibid.

the smooth operation of the infrastructure. The methodology for risk assessment of critical infrastructure was adopted and the characterization of critical infrastructure systems was included and the authorities responsible for their protection were identified. The method of cooperation between the public and private sectors at the strategic and operational level was described. The guidelines for critical infrastructure protection exercises and research and development projects on this subject have also been taken into account.

2. Legal aspects of the protection of national and European critical infrastructures

The legal basis for identification and protection of the systems of national and European critical infrastructure in the territory of Poland are the provisions of the aforementioned Act on crisis management. Critical infrastructures receive considerable attention in this document, ranging from their detailed definition and the exhaustive listing of eleven of their systems, through their protection tasks, to issues related to critical infrastructures in the European Union.

Under the Act, the duty to protect critical infrastructure rests with public administration bodies, independent or dependent owners and holders of such infrastructure. Tasks implemented by these entities include: 1) collecting and processing information on threats to critical infrastructure; 2) preparing procedures to deal with such threats; 3) restoring critical infrastructure; and 4) cooperating with entities in charge of its maintenance in the field of critical infrastructure protection. A person should be personally appointed by the owner or holder of the critical infrastructure's facilities, installations or equipment to maintain contact with the entities competent for the protection of critical infrastructure. In addition to the obligation to protect critical infrastructure, the legislator obliges the owners and holders of critical infrastructure to maintain their own back-up systems to ensure security and sustain the operation of the infrastructure until it has been fully restored. They are also obliged to prepare and implement plans for the protection of CI, in accordance with the expected threats, while the tasks related to the prevention, mitigation and elimination of the effects of terrorist events should be performed in cooperation with government administration bodies competent in these matters, in particular the Head of the Internal Security Agency[16]. Detailed guidelines on the method of establishment, updating and content of critical infrastructure protection plans – developed by their owners and holders (hereinafter referred to as "critical infrastructure operators") – are set out in the Regulation of the Council of Ministers of 30 April 2010 on critical infrastructure protection plans[17].

[16] *Act of 28 April 2007 on crisis management...*, op. cit., art. 6 and 12a.
[17] Journal of Laws of 2010 No. 83, item 542.

At different levels of crisis management, the characterization of threats to critical infrastructures and their risk assessment are included in the Master Crisis Management Plan, while functional annexes to the Master Plan specify, inter alia: 1) procedures for the implementation of tasks related to the protection of critical infrastructure; 2) list of critical infrastructure located respectively in the province, county or commune covered by the crisis management plan; 3) priorities in the field of protection and restoration of critical infrastructure[18].

In order to create the conditions for improving the security of critical infrastructure, the legislator instructed the Council of Ministers to adopt the National Program for Critical Infrastructure Protection, mentioned in the previous subchapter. The legislator made the Director of the Government Security Center the main executor of the NPCIP, and the entities cooperating in the preparation of this document – ministers and heads of central offices responsible for critical infrastructure systems and competent in matters of national security. At the same time, it was noted that the program was to be updated at least once every two years. The Act empowers the Council of Ministers to define – by way of a regulation – the manner of implementation of obligations defined in the Act and cooperation in the field of NPCIP by public administration and services responsible for national security with the owners and holders of CI facilities, installations, equipment and services[19]. This task materialized through the issuance of the Regulation of the Council of Ministers of 30 April 2010 on the National Program for Critical Infrastructure Protection[20].

The Regulation specifies how public administration bodies perform their duties within the scope of the National Program for Critical Infrastructure Protection and how they should cooperate with operators of critical infrastructure in this respect, i.e. with its owners or holders. The Regulation obliges the Director of the Government Security Center to develop criteria for the identification of critical infrastructure and to reconcile these criteria with the ministers and heads of central offices responsible for these systems. The criteria shall, when reconciled, form the basis for the preparation of a proposal for an inventory of critical infrastructures. Proposals to this effect shall be made by the above-mentioned Ministers and Heads of Central Offices responsible for critical infrastructure systems and verified by the Director of the Government Security Center[21]. The regulation also stresses the important role of ministers and heads of central offices in the process of preparing the National Program for Critical Infrastructure Protection. They shall be the main coordinators in creating the conditions for enhancing the security of critical infrastructure within the system.

---

[18] Act of 28 April 2007 *on crisis management...*, op. cit., art. 5.

[19] Ibid., art. 5b.

[20] Journal of Laws of 2010 No. 83, item 541.

[21] Regulation of the Council of Ministers of 30 April 2010 *on the National Program for Critical Infrastructure Protection...*, op. cit., art. 1-4.

Information and proposals received from ministers and heads of central offices are the basis for the development of the Program for Critical Infrastructure Protection, which is presented for approval by the Council of Ministers[22].

Pursuant to the Act on Crisis Management and the provisions of the Regulation on the National Program for Critical Infrastructure Protection, the Director of the GSC shall establish a consolidated list of critical infrastructure facilities, installations, equipment and services broken down by system. Extracts from this list shall be forwarded, according to their competence, to the competent ministers and heads of central offices. In turn, province governors receive extracts containing facilities, installations, equipment and services forming critical infrastructure located in the province. The list of critical infrastructures, as well as the whole *Program*... shall be updated at least every two years[23].

3. Tasks of government administration in the field of critical infrastructure protection

Critical infrastructure protection is the responsibility of all individual and collective actors in a state. Hence, the National Program for Critical Infrastructure Protection is addressed to: public administration bodies at all levels of management, operators of critical infrastructure, entrepreneurs, the scientific community and the society. Above all, however, the program is addressed to CI operators and government administration. "The main addressees of the Program in the government administration are the ministers responsible for critical infrastructure systems and province governors. The program is also addressed to other administrative bodies, institutions and entities"[24]. The coordination of critical infrastructure protection processes is carried out by the Government Security Center.

The Government Security Center[25] is a state budget unit subordinate to the Prime Minister. In matters of crisis management, it provides services to: the Council of Ministers, the Prime Minister, the Government Crisis Management Team and the minister in charge of internal affairs. The GSC acts as the national crisis management center, carries out continuous threat monitoring and is on duty as part of the State's defense preparedness. The Center's main tasks include central civilian planning and preparation of the launch of crisis management procedures. The GSC develops threat

[22] Ibid., art. 5-6.

[23] Ibid., art. 10-11.

[24] *National Program for Critical Infrastructure Protection*, Government Security Center, Warsaw 2015, p. 11.

[25] The organization and detailed tasks of the Government Security Center are defined in the Regulation of the Prime Minister of 11 April 2011 on the organization and mode of operation of the Government Security Center, Journal of Laws of 2011 No. 86, item 471.

characterization and risk assessment, including for critical infrastructure. The Center coordinates the information policy of public administration bodies in a crisis situation and is responsible for ensuring the circulation of information between domestic and foreign bodies and structures in crisis management. The Center also organizes and conducts training and exercises nationwide and participates in international exercises. The GSC carries out critical infrastructure protection planning tasks, including developing and updating a functional annex to the National Crisis Management Plan and acts as the National Focal Point within the European Union and NATO[26].

In the preparation of the National Program for Critical Infrastructure Protection, the Government Security Center plays a key role, which has already been mentioned. The document itself defines a number of tasks for this entity, which make the Center "play a key role in building a critical infrastructure protection system based on shared responsibility, cooperation and trust"[27]. These include: 1) building partnerships, organizing and developing networks for the exchange of information between program participants; 2) developing and implementing methodologies for assessing the risk of disruption to critical infrastructure; 3) carrying out, in cooperation with the Ministers responsible for the different CI systems, a risk analysis of crises caused by the disruption of the CI systems; 4) developing support mechanisms for the restoration of critical infrastructure; 5) assessing the continued effectiveness of the program. Moreover, the GSC carries out a number of informational and educational projects related to the functioning of the NPCIP in the public space and initiates and supports scientific research and development works related to the protection of critical infrastructure[28].

The **ministers** responsible for critical infrastructure systems, in the light of the "National Program for Critical Infrastructure Protection", are a guarantee "of the involvement of the highest state authorities in the process of building state security. Taking into account the adopted model of critical infrastructure protection, each CI system needs a host with the best knowledge of the system and who understands its design and the needs of the actors involved. The ministers in charge of government administration departments or task areas comparable to CI systems are best prepared on the part of the administration to perform this role"[29]. The following are responsible for the individual critical infrastructure systems in Poland:

- Ministers: of the Economy and of the Treasury (each according to their own competencies) for the energy, energy resources and fuel supply systems;
- Minister of Administration and Digitization for the communication system and ICT networks system, as well as for the systems ensuring continuity of public administration operations;

[26] T. Szczurek, *Od deskrypcji do antycypacji…*, op. cit., p. 245.
[27] *National Program for…*, op. cit., p. 13.
[28] Ibid., pp. 13-14.
[29] Ibid., p. 17.

- Minister of Finance for the proper functioning of the State's financial systems;
- Minister for Agriculture and Rural Development for food supply systems;
- Minister of Health for the health care system;
- Minister for Transport, Construction and Maritime Affairs for transport systems;
- Minister of the Interior for emergency systems;
- Minister for the Environment, for the systems of production, warehousing and storage of chemical and radioactive substances, including pipelines of hazardous substances, and (together with the Minister for Administration and Digitization) for the systems of water supply[30].

Ministers and heads of central offices, under the responsibility for supervised critical infrastructure systems: 1) coordinate the cooperation between critical infrastructure operators; 2) ensure the exchange of information between public administrations and these operators; 3) submit information to the Director of the Government Security Center on the characteristics of the area of responsibility under their jurisdiction; 4) identify the resources of this area in terms of critical infrastructure protection needs; 5) propose requirements and standards to ensure the continuous functioning of the critical infrastructure; 6) present an overall risk assessment on the functioning of this area, taking into account vulnerabilities and potential consequences in case of malfunctions of the critical infrastructure in this area; 7) present possible ways of preventing disruptions to the functioning of the task area due to damage to critical infrastructure; 8) propose the adoption of relevant priorities for the restoration of damaged or destroyed infrastructure.

The Minister of National Defense was not mentioned as one of the ministers responsible for the various critical infrastructure systems in the NPCIP. It should be borne in mind, however, that this minister is responsible for protecting facilities that are particularly important for the security and defense of the state and which are part of the national security infrastructure[31]. Other Ministers and Heads of Central Offices with crisis management responsibilities – but who are not responsible for specific critical infrastructure systems – are required to support and cooperate with the parties involved in information sharing, research and development programs. In general, the whole Council of Ministers is involved in the implementation of the National Program for Critical Infrastructure Protection.

[30] Ibid., p. 18. *In the event that responsibility for the system rests between more than one minister, each of the co-hosts shall perform the above-mentioned tasks in relation to those facilities which have been agreed upon with the other co-hosts.* (Ibid., p. 18)

[31] More in: J. Padzik, *Prawnoustrojowa pozycja ministra obrony narodowej w systemie organów administracji rządowej*, [in:] „Bezpieczeństwo Narodowe", Kwartalnik Biura Bezpieczeństwa Narodowego, no. 4/2011, Warsaw 2011, pp. 95-104.

Governors representing the government on the ground play an important role in the critical infrastructure protection system[32]. The tasks of a provincial governor in matters of crisis management include: counteracting threats in the province, preparing a provincial crisis management plan and – which is most important from the point of view of the subject under consideration – protecting critical infrastructure. Moreover, the provincial governor approves county crisis management plans and is responsible for conducting exercises, workshops and trainings on the components of the crisis management system in the province. In the area of prevention, counteraction and removal of the effects of terrorist events – also in the area of counteracting threats to critical infrastructure located in the province – the provincial governor cooperates with the Head of the Internal Security Agency. It is the responsibility of the provincial governor to request the use of sub-divisions or divisions of the Armed Forces of the Republic of Poland to perform anti-crisis tasks, including the implementation of tasks in the event of threats to critical infrastructure. A significant part of critical infrastructure protection projects in the province is also carried out by: the police, fire brigade and other joint services, inspections and guards[33].

In order to achieve the objectives of the National Program for Critical Infrastructure Protection, provincial governors organize and operate a provincial forum for critical infrastructure protection, cooperate with local governments in the administered area (the Marshal of the Province, starosts, heads of villages, mayors, city mayors) and with the CI operators in the field of counteracting disruptions to the functioning of critical infrastructure. By preparing and updating the Interim Report on National Security Threats, province governors actively participate in the process of assessing the risk and occurrence of a crisis situation in the state caused by the destruction or disruption of critical infrastructure located in the province. "The provincial level is the point of transition between the systemic and territorial approach to critical infrastructure protection, and the services, guards and inspections subordinate to provincial governors are an important element of planning in the event of disruption of the CI located in the territory of the province"[34].

4. Critical infrastructure protection in the European Union

Both the privileges and duties resulting from membership in the European Union translate into all spheres of public life in the Member States. It should be remembered that, in general, the national interests of individual societies must give way to the interests of the community and that the regulations of EU law take precedence over

[32] Ibid., p. 23.
[33] T. Szczurek, *Od deskrypcji do antycypacji…*, op. cit., p. 248.
[34] *National Program for…*, op. cit., p. 23.

national law[35]. Admittedly, these interests seem to be fully converging in the field of critical infrastructure protection.

The European Council[36] already called for the preparation of an overall strategy for the protection of critical infrastructure in June 2004. "In December 2005, the Justice and Home Affairs Council invited the Commission to prepare a proposal for a European Program for Critical Infrastructure Protection ("EPCIP") and decided that the program should be based on an all-hazards approach, while addressing terrorist threats as a priority"[37]. The identification of terrorist threats as a priority was undoubtedly the aftermath of the memorable attacks on the World Trade Center and Pentagon on 11 September 2001, when nearly 3,000 people were killed. In Europe, wounds were treated after the terrorist attack on suburban trains in Madrid on 11 March 2004. Almost 200 people were killed and more than 1.2 thousand injured in this attack[38].

In 2007, the Council[39], as the main EU decision-making body, adopted conclusions on the European Program for Critical Infrastructure Protection, underlining that the primary responsibility for protecting critical infrastructure rests with the Member States, owners, operators and users, users being defined as organizations which operate and use the infrastructure for economic purposes and for the provision of services[40]. Council Directive of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection defines critical infrastructure as an asset, system or part of an infrastructure located in the territory of EU Member States, where that system or elements of the system are essential for the maintenance of vital social functions, health, safety, security, material or social well-being of people and where

[35] It is the duty of each Member State of the European Union to implement (incorporate into its own legal system) the *acquis communautaire*, covering the so-called "primary law" (founding treaties, accession treaties and international agreements which amended these treaties) and "secondary law" comprising of: (1) the provisions issued by the bodies of the Union on the basis of the said Treaties, (2) the international agreements concluded by the EU, (3) the case law of the Court of Justice, (3) the declarations and resolutions and (4) the general principles of Community law.

[36] It should be noted that the European Council (currently one of the seven official EU institutions) does not have the power to legislate. Its role is to set out the EU's general policies and priorities.

[37] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of EU L. 375/75, recitals to the document, point (3).

[38] T. Szczurek, *Od deskrypcji do antycypacji…*, op. cit., p. 178.

[39] This refers to the 'Council of the European Union', which is referred to as the 'Council" in legal acts, because until 30 November 2009 it was officially not an EU body but an "European Community body".

[40] Council Decision of 12 February 2007 establishing for the period 2007-2013, as part of the General Program on Security and Safeguarding Liberties, a specific program: *Prevention, preparedness and management of the consequences of terrorism and other security-related risks*, Official Journal of EU L. 07.58.1, point 10.

their disruption or destruction would have a significant impact on a Member State as a result of the loss of those functions[41]. Energy and transport sectors have been identified as a priority for European Critical Infrastructures and should be reviewed as a matter of priority to assess the impact of their disruption. The European Program for Critical Infrastructure Protection itself has identified further sectors relevant to Community security, including information and communication technology (ICT).

In the context of EU legal regulations, the definition of critical infrastructure – specified in the Polish Act on crisis management – is fully compatible with the Council Directive. After the aforementioned amendment of 17 July 2009, point 2a was introduced to Art. 2 of the same Act, where European critical infrastructure is defined as systems and their constituent functional objects, including construction works, equipment and installations which are essential for the security of the state and its citizens and serve to ensure the efficient functioning of public administration bodies, as well as institutions and businesses, designated in energy supply systems, energy and fuel resources and in transport systems for electricity, oil and natural gas and for transport by road, rail, air, inland waterways, ocean, short sea shipping and ports, situated in the territory of Member States of the European Union, the disruption or destruction of which would have a significant impact in at least two Member States[42].

In the opinion of the authors of the National Program for Critical Infrastructure Protection, this program and the whole range of critical infrastructure protection activities carried out at the national level correspond well with the broad European context. *Poland actively participates in EPCIP projects. The role of the coordinator of these activities, as the national contact point, is performed by the Government Security Center*[43].

Summary

Critical infrastructure protection is one of the most important projects carried out to ensure national and international security. Public administration plays a very important role in the protection of critical infrastructure. Special tasks – with regard to the selection of facilities, equipment, installations and services crucial for the security of the state and citizens and the assessment of the risk of threats to this infrastructure – lie with the ministers responsible for particular systems. The National Program for Critical Infrastructure Protection is a coherent document which comprehensively covers the prevention and counteraction of threats, response to their occurrence and restoration of critical infrastructure. A key role in this respect is assigned to the Government Security Center, which prepares a draft program and

[41] Council Directive 2008/114/EC of 8 December 2008 on the recognition and designation of ..., op. cit., Article 2, point a.
[42] *Act of 28 April 2007 on crisis management*..., op. cit., art. 3, point 2a.
[43] *National Program for…*, op. cit., pp. 47-48.

coordinates all projects related to its implementation, including cooperation within the European Union.

REFERENCES

1. Act of 17 July 2009 amending the Act on crisis management, Journal of Laws of 2009 No. 131, item 1076.
2. Act of 28 April 2007 on crisis management, Journal of Laws of 2007, No. 89, item 590, as amended.
1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of EU L. 375/75.
3. Kitler W., *Bezpieczeństwo Narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Akademia Obrony Narodowej, Warsaw 2011.
4. Kitler W., *Funkcje i zadania władzy wykonawczej w dziedzinie bezpieczeństwa narodowego*, [in:] W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP – część ogólna*, Akademia Obrony Narodowej, Warsaw 2013.
5. *National Program for Critical Infrastructure Protection*, Government Security Center, Warsaw 2015.
6. *National Security Strategy of the Republic of Poland*, Warsaw 2007.
7. Padzik J., *Prawnoustrojowa pozycja ministra obrony narodowej w systemie organów administracji rządowej,* [in:] „Bezpieczeństwo Narodowe", Kwartalnik Biura Bezpieczeństwa Narodowego, no. 4/2011, Warsaw 2011.
8. Pyznar M., *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa*, [in:] A. Tyburska (ed.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010.
9. Radziejewski R., *Jak ocenić (zmierzyć) bezpieczeństwo kluczowej infrastruktury państwa?*, [in:] M. Cieślarczyk, A. Filipek, A.W. Świderski, J. Ważniewska (ed.), *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, vol. 1, Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2013.
10. Regulation of the Council of Ministers of 30 April 2010 on the National Program for Critical Infrastructure Protection, Journal of Laws of 2010 No. 83, item 541.
11. Regulation of the Council of Ministers of 30 April 2010 on the plans for Critical Infrastructure Protection, Journal of Laws of 2010 No. 83, item 542.
12. Regulation of the Prime Minister of 11 April 2011 on the organization and mode of operation of the Government Security Center, Journal of Laws of 2011 No. 86, item 471.
13. Skomra W., *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, [in:] A. Tyburska (ed.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010.
14. Surmański M., *Bezpieczeństwo i obronność państwa w świetle kompetencji Prezydenta RP i Rady Ministrów*, [in:] „Bezpieczeństwo Narodowe", Kwartalnik Biura Bezpieczeństwa Narodowego, no. 1/2013, Warsaw 2013.

15. Szczurek T., *Od deskrypcji do antycypacji wykorzystania potencjału militarnego w kształtowaniu bezpieczeństwa nowoczesnych wspólnot państwowych wobec rozwoju zagrożeń niemilitarnych*, Wydawnictwo Wojskowej Akademii Technicznej, Warsaw 2012.
16. Tyburska A., *Ochrona infrastruktury krytycznej w Polsce – wyzwania w tworzeniu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warsaw 2013.

OCHRONA NARODOWEJ I EUROPEJSKIEJ INFRASTRUKTURY KRYTYCZNEJ

Streszczenie. Ochrona krajowej i europejskiej infrastruktury krytycznej na terytorium Rzeczypospolitej Polskiej jest złożonym procesem wymagającym wysiłków wielu instytucji publicznych i prywatnych. W szczególności właściciele i użytkownicy systemów infrastruktury krytycznej są zobowiązani do zapewnienia takiej ochrony. Są to kluczowe obowiązki z punktu widzenia bezpieczeństwa narodowego, ponieważ zniszczenie, uszkodzenie, złe działanie lub jakiekolwiek inne ograniczenie funkcjonowania infrastruktury krytycznej może stanowić poważne zagrożenie dla funkcjonowania społeczeństw w skali lokalnej, krajowej, a nawet europejskiej. Rzeczywiście wiele systemów obejmuje więcej niż jeden kraj. Nawet jeśli infrastruktura znajduje się w państwie członkowskim Unii Europejskiej, ale jej zakłócenie lub zniszczenie miałoby znaczny wpływ na co najmniej dwa państwa członkowskie, jest klasyfikowane jako „krytyczna infrastruktura Unii Europejskiej". W Polsce infrastruktura krytyczna to jedenaście systemów obejmujących urządzenia, sprzęt, instalacje i usługi kluczowe dla bezpieczeństwa państwa i obywateli. Operatorzy tej infrastruktury są zarówno podmiotami państwowymi, jak i prywatnymi właścicielami, jednak właściwi ministrowie i szefowie urzędów centralnych odpowiadają za poszczególne systemy na poziomie krajowym. Narodowy Program Ochrony Infrastruktury Krytycznej jest ważnym dokumentem regulującym kwestie ochrony infrastruktury krytycznej w Polsce. Głównym celem programu było stworzenie warunków dla poprawy bezpieczeństwa infrastruktury krytycznej, obejmującej wszystkie cztery fazy zarządzania kryzysowego: zapobieganie zakłóceniom, gotowość na sytuacje awaryjne, reagowanie w sytuacjach kryzysowych i przywracanie zniszczonej infrastruktury krytycznej. Zgodnie z ustawą o zarządzaniu kryzysowym dyrektor Centrum Bezpieczeństwa Rządu jest osobą odpowiedzialną za koordynację wszystkich projektów i głównego wykonawcę projektu programu. Szczegółowe informacje na temat infrastruktury krytycznej przygotowywane są przez ministrów odpowiedzialnych za te systemy. Program wchodzi w życie po zatwierdzeniu projektu przez Radę Ministrów. Wszystkie poziomy administracji publicznej są zaangażowane w realizację zadań zawartych w Krajowym Programie Ochrony Infrastruktury Krytycznej. Związane jest to przede wszystkim z obowiązkami administracji rządowej i samorządowej w obszarze (sfera) zarządzania kryzysowego. Pierwszy program w Polsce został wprowadzony 30 kwietnia 2010 r. na podstawie odpowiedniego rozporządzenia Rady Ministrów. Program jest aktualizowany co najmniej co dwa lata. Wersja 2015 jest dostępna na stronie internetowej Rządowego Centrum Bezpieczeństwa. Następna wersja tego dokumentu będzie dostępna wkrótce.
Słowa kluczowe: bezpieczeństwo, bezpieczeństwo narodowe, bezpieczeństwo regionalne, infrastruktura, infrastruktura krytyczna, Narodowy Program Infrastruktury Krytycznej.