„Polityka i Społeczeństwo" 2(20) / 2022
DOI: 10.15584/polispol.2022.2.1

ARTYKUŁY

Marek Barć*

PLANNING AND ORGANISING PROTECTION OF CRITICAL INFRASTRUCTURE

Abstract

The article is devoted to planning and organizing critical infrastructure protection. The planning method was indicated there, and the layout of the critical infrastructure protection plan was presented. The most important thing is to protect critical infrastructure components that citizens use on a daily basis. So in the article I am talking about energy supply systems, energy resources and fuels, food and water supply system. And above all about financial systems, healthcare and ICT.

Key words: critical infrastructure, protection, security system, protection plan

Introduction

Place and role of critical infrastructure in our social life seems to be noticed by politicians and policy-makers even during crisis, because it is seen as a starter of economical growth. It is hoped that ideas included in the Government Strategy for National Security System Development will not be treated as a project but they will be put into practice, as their authors noticed, that a characteristic feature of highly developed societies is access to services providing living standards accepted as elementary.

Legal basis for critical infrastructure protection

The term critical infrastructure[1] is a quite young wording, because it was spread out in the 90s of the 20th century. At that time there were

* Politechnika Rzeszowska, e-mail: mbarc@prz.edu.pl, ORCID: 0000-0001-7379-8576.

[1] Critical infrastructure is, according to the Act on Crisis Management, systems and their functionally related objects, including construction objects, devices, installations, key services for the security of the state and its citizens and to ensure the efficient functioning of public administration, as well as institutions and entrepreneurs.

many serious cases of blackout in the USA thus they caused many difficulties to millions of inhabitants. Such events are typical for high-tech developed countries with dense energetic network and they do not occur only in the USA but also in other countries and Poland[2] itself. Blackout in Poland in the surrounding area of Szczecin in winter in 2009 is the example of such actions[3], because Szczecin agglomeration was not provided with electricity for many days[4]. The term mentioned previously with the change of the issue of danger , especially increase of risk of terrorism, the area connected with this term has been broadened with new countries' infrastructure systems. In June 2004 the European Council assessed dangers to main systems and installations of European security and ordered preparation of general strategy for safety of European critical infrastructure. The outcome of such actions were issued notices covering proposals directed to making critical infrastructure security systems more efficient in preventing them from terrorist attacks. In 2005 the so called "green book"[5] was accepted, which included political options dealing with preparing a security programme and a system warning about dangers for critical infrastructure system[6].

Another step on the road to minimise danger to critical infrastructure was a proposal of The Justice and Home Affairs Council to create European Critical Infrastructure Protection Program (ECRPP). This program was to cover all kinds of dangers, i.e. man-made, natural (those caused by nature forces), technological mainly focused on terrorism. In 2007 the European Commission, consulting current arrangements, indicated that the main responsibility for protection of critical infrastructure belongs to

[2] *Critical Infrastructure Protection III,* eds. Ch. Palmer, S. Shenoi, New York 2009.

[3] They caused the failure of the power system in the area of the Szczecin agglomeration extreme rainfall under special wet snow deposition conditions on line conductors and other components.

[4] See more: K. Michalski, M. Jurgilewicz, *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Warszawa 2021.

[5] The main aim of the Green Paper is to inform about possible EPCIP policy options by involving a large number of stakeholders. Effective protection of critical infrastructure requires communication, coordination and cooperation at national and EU level between all stakeholders - infrastructure owners and operators, regulators, professional organizations and industry associations - in cooperation with all levels of government and the public at large. The Green Paper provides information on how the Commission can respond to the Council's request for the establishment of EPCIP and CIWIN and is the second phase of the consultation process for establishing a European Critical Infrastructure Protection Program. The Commission expects to receive concrete information on the policy options described in this document by presenting this Green Paper.

[6] The Commission of The European Communities, Brussels 17th November 2005, Com. (2005).

Member States, owners, operators and users[7]. The consequence of further actions was a directive of the European Council specifying rules for recognising and determining European critical infrastructure[8]. Due to arrangements in 2007 Poland started actions which were connected with establishing National Critical Infrastructure Protection Plan, which should create general frames for determining and protecting chosen systems and objects of critical infrastructure.

a) Legal regulations concerning critical infrastructure protection

Legislative solutions concerning critical infrastructure were incorporated in the Act about crisis management dated on 26th April 2007[9]. It does not mean that this problem was perceived after the attempt of the European Council emphasizing creation of National Critical Infrastructure Protection Plan. In Polish legislation the problem about protection of objects with significant role for national security and economy was included in the Persons and Property Protection Act dated August 22nd, 1997[10] and in the Regulation of the Polish Council of Ministers of June 24th, 2003[11]. The data included in the documents do not respond directly to critical infrastructure, but the analysis of terms used referring to enumerated objects reflects similar meaning[12].

The Act on protection of person and property also indicates objects classified to compulsory protection. In the 5th article of this Act there are

[7] The Council Decision on 2nd February 2007 establishing for 2007-2013 as a part of a general programme – detailed programme dealing with security a protecting people. *Preventing, readiness and managing results of terrorism and other kinds of risk for security*. (Official Journal UET) dated on 2007, No 58, position 1, point 10.

[8] The Council Directive 2008/114 WE dated on 8th December 2008 (Official Journal EU) dated on 2008, No 345, position 75.

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

[10] Act of August 22, 1997 on the protection of persons and property. (Journal of Laws of 1997, No. 114, item 740, as amended).

[11] Regulation of the Council of Ministers of June 24, 2003 on objects of particular importance for state security and defense and their special protection (Journal of Laws of 2003, No. 116, item 1090).

[12] See more eg. K. Zieliński, *Ochrona ludności. Zarządzanie kryzysowe*, Warszawa 2021; S. Rysz, *Zarządzanie kryzysowe zintegrowane*, Warszawa 2020; M. Jurgilewicz, *Rola podmiotów uprawnionych do użycia lub wykorzystania środków przymusu bezpośredniego i broni palnej w ochronie bezpieczeństwa i porządku publicznego*, Siedlce 2017.

enumerated areas, objects and devices important for defense, country's economic interests, widely perceived security and other important objects which are protected by special formations. Comparison of those mentioned in the Act, i.e. areas, objects and devices that undergo compulsory protection with systems and included in the repository functionally connected objects mentioned in the Act for crisis management as critical infrastructure objects indicates that the legislator thinks of the same objects and devices. We might have similar impression analyzing the regulation of the Council of Ministers dealing with objects especially important for security and defense (being an implementing act to the Act on Universal Duty to Defend the Republic of Poland), which categories objects as those of first and second category and tasks of their particular protection. Objects and devices mentioned in this Act mostly correspond to description of critical infrastructure objects stated in the Act for crisis management mentioned previously. All objects are protected but the legislator has not described forms of its protection. The analysis of statuary obligation mentioned previously indicates that objects enumerated in these Acts should be protected according to separate rules whereas it concerns the same objects[13].

There is discrepancy about subjects running security tasks. The Regulation of the Council of Ministers on the structures especially important for the national security and defense states that "specific protection of objects shall be carried out by militarized forces especially formed for this case, saved as the otherwise provided[14]." It is thought that they will be created in case of threat for national security, but for a different case the indication of a subject misses that shall protect. Specific Armed Security Forces (SASF) are mentioned in the Act on protection of person and property as additional subjects to protect objects of sensitive protection.

b) The EU documents

Law regulations concerning determining and protection of critical infrastructure were both included in national and European documents. The basic document mentioned earlier is The Council Directive

[13] M. Jurgilewicz, A. Dana, *Prywatyzacja bezpieczeństwa i porządku publicznego – specjalistyczne uzbrojone formacje ochronne* [w:] *Państwo. Prawo. Bezpieczeństwo,* tom III, red. A. Babiński, M. Jurgilewicz, N. Malec, Szczytno 2017, pp. 45-66.

[14] Regulation of the Council of Ministers of June 24, 2003 on objects of particular importance for state security and defense and their special protection (Journal of Laws of 2003, No. 116, item 1090).

2008/114 WE[15] dealing with meeting and determining European critical infrastructure and estimating the needs in the scope of its protection improvement. This document also states that "on the territory of community there is a number of critical infrastructures whose interruption or destruction would have cross-border effects." It mainly deals with intersector effects being the outcome of mutually connected infrastructures. Such an European Critical Infrastructure (ECI) shall be recognized and assigned by a mutual procedure. Rules and guidelines included in this directive were supposed to have been incorporated by January 12, 2011[16]

c) National documents

Provision of the European Directive made the fact that in the Law of the management of crisis a number of solutions coherent with the Council were accepted. The definition of European critical infrastructure [17](ECI) was stated in it, rules for creating a unitary list of objects, installations, facilities and services being a part of critical infrastructure which is dislocated on the Polish territory and has an influence on border countries and European critical infrastructure located on the territory of other EU Member States and also defining demands for classifying this infrastructure according to sector and horizontal criteria. The Government Centre for Security was chosen for a competent institution. The Head of this Centre was made a person responsible for preparing a proposal of CI for ECI and also informing the European Commission on timely manners (every year) about a number of critical infrastructures which were discussed to be qualified CI objects as ECI. The Law imposes a duty to accept National Programme for Critical Infrastructure Protection by the Council of Ministers, which is aimed at making conditions to improve security of critical infrastructure especially: 1) preventing from function-

[15] COUNCIL DIRECTIVE 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection.

[16] Member States shall adopt the necessary provisions to implement this Directive by 12 January 2011. They shall forthwith inform the Commission thereof and communicate to it the text of those provisions and a correlation table between those provisions and this Directive.

[17] European Critical Infrastructure or ECI means critical infrastructure located on the territory of the Member States, the disruption or destruction of which would have a significant impact on two or more Member States. Whether the impact is significant is assessed against the cross-cutting criteria. This includes effects resulting from cross-sector interdependencies with other types of infrastructure.

al disturbances of critical infrastructure; 2) preparing for crisis situations which may influence badly on critical infrastructure; 3) reacting to destruction or distortion of critical infrastructure; 4) rebuilding critical infrastructure. The program defines: national priorities, goals, requirements and standards aimed at proper functionality of critical infrastructures; ministers managing departments of government administration and managers of central authorities responsible for CI systems and objects; specific criteria allowing to separate objects, installations, devices and services being a part of critical infrastructures systems, taking into account their significance for country's functionality and cater the needs of citizens[18].

The Director of Government Centre for Security is assigned as the executive of these actions who is obliged to cooperate with ministers, managers of central authorities, voivods and people responsible for systems. What is more, the executive is responsible for preparing the mentioned document. Law regulations dealing with the scope of the CI plan adjusts the Act of the Council of Ministers to the issued act. This act defines both the way of creating and structure of protection of critical infrastructure by owners and independent and subsidiary object users, installations critical infrastructure devices.

Another act that regulates the cases of protection of critical infrastructures is the The Regulation of the Council of Ministers on National Critical Infrastructure Protection Program (NCIPP)[19]. The Act states goals for the director of Government Centre for Security (GCS) aiming at working out criteria for directors of central authorities about making proposals for determining critical infrastructure and dates and information including: 1) characteristics for the area assigned to them, dealing with identifying the sources, subsystems, functions and correlation with other critical infrastructure systems, 2) proposals for criteria and standards allowing to provide continuity of critical infrastructure actions, 3) general risk estimation for functioning of the assigned task area, including threats, capacity to risk and consequences for interference of critical infrastructure, 4) priority proposals for rebuilding critical infrastructure, 5) possible ways for preventing from disturbances in functioning of task area resulting from disturbing the function of critical infrastructure, 6) proposals for research and development programs that may increase safety on critical infrastructure[20].

[18] National Programme for Critical Infrastructure Protection.

[19] Regulation of the Council of Ministers of 30 April 2010 on plans for protection of critical infrastructure (Official Journal dated 2010 No 83, position 542.

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

Improvement for critical infrastructure security has been proposed by: 1) realisation of appointed priorities and goals of the program, 2) providing conditions for improving security in scope of continuity of functioning of critical infrastructure, 3) being prepared for crisis situations that may be the outcome of critical infrastructure interruption or may influence the infrastructure negatively, 4) being ready to react in case of destruction or when critical infrastructure functioning is interrupted, 5) providing conditions for rebuilding critical infrastructure, 6) comply with standards and criteria included in the program,7) cooperation in implementing the Program[21].

Preparation and running protection of critical infrastructure objects

Protection of critical infrastructure is a number of numerous actions leading towards providing functionality and continuity of actions for critical infrastructure integrity due to prevent from dangers, risks and weak points and also reduction and neutralization their effects, and rebuilding quickly this infrastructure in case of breakdown, attacks and other events interrupting its proper function[22]. Hence, if we want to protect infrastructure effectively perceived as critical its functionality must be provided when facing different threat categorized as natural (floods, fires, hurricanes, low temperatures or heat) or man-made (negligence of device inspection, destruction of devices both unconsciously or consciously). The question is how we can prepare and perform protection of systems and critical infrastructure objects when it is hard to point at homogenous forms and ways of protection due to their varied character or specific threats.

a) General rules for protecting objects

The term "object" means a building or a set of buildings and facilities placed on a certain area. The need to secure such defined objects may result from many normative documents[23] and leads to physical security and technical protection. We cannot talk about exhaustion of condi-

[21] *Ibidem*.

[22] The Act for crisis management, article 3, point 3.

[23] The Act for crisis management, The Act on Universal Duty to Defend the Republic of Poland, The Regulation of the Council of Ministers of 24th June 2003 on the structures especially important for the national security and defence.

tions for complex protection of critical infrastructure, which of these may be enumerated: physical protection (limited access of a third party); technical protection (following building regulations, fire prevention regulations, etc.); personal security (limited access to people with security clearance); ICT protection (protecting control system and data transmission from cyber-terrorism); legal protection (preventing a CI object from hostile action – on doing business); supporting rebuilding phase (government guarantees, actions taken to shorten the time necessary to recover functions of critical infrastructure)[24].

Protection of an object is a set of administrative, tactical, technical and physical tasks preventing from crimes and offence against it and prevents from further damages as the outcome of these actions avoiding occurring damage resulting from these actions and avoiding the entrance of unauthorized staff to the protected object[25]. Internal protection covers the protected object. The number of zones depends on a number of protected objects (buildings) in the system. The zone includes interior of an object and external walls with holes (doors, windows). External protection is the area outside the building to the fence or the boundary of the site. Peripheral protection covers the area either outside the fence or the boundary site. This zone is settled down when the protected object is placed further from compact urban settings and presence of unauthorized staff is not prohibited there. Internal protection zone should be focused on protecting object interior from threats, i.e., both internal and external. Other security zones are especially prepared in case of external threats[26].

Internal threats are mainly caused by object employees and result from unlawful actions, i.e. thefts, aimed damage or breakage of devices placed in the object, gaining sensitive information and passing it out of the site. External threats are mainly burglaries aimed at destroying technical devices or computer programs, power supply breakage leading to failure of devices or installations, explosion, etc.. Criminal activities categorized as external or internal can be done as individual or organized criminal group actions. Physical protection is done by Specific Armed Security Forces (SASF), perceived as internal security forces or entrepreneurs that received permission to do business aiming at services, pro-

[24] M. Pyznor, *National Programme for Critical Infrastructure Protection – conference materials. Critical Infrastructure Protection – the assessement of the need and abilities*, Szczytno 2010, p. 25.

[25] The Act on protection of person and property, art. 2, point 5.

[26] The Act on Crisis Management, the Act on the Universal Duty of Defense of the Republic of Poland, the Regulation of the Council of Ministers on objects of particular importance for state security and defense and their special protection of June 2004.

tection of person and property[27]. The second is for technical protection aiming at: installing electronic regulations and alarm systems informing about threats to protected objects, exploitation, maintenance, repairs in places of installation; and assembling devices and means of mechanical protection and their exploitation, maintenance and repairs and emergency opening in places of their installation[28].

b) Planning protection of critical infrastructure objects

Protection of critical infrastructure is based on preparing and implementing it. The preparation includes planning and organizing activities. Planning includes the actions concerning planning and organizing. Planning is aimed at working out ideas for an action (making a decision), which include: a) task analysis, b) estimating the object and its surrounding area, c) analysis and hazard assessment, d) assessing forces and means, e) estimating changes in the object.

c) Object protection plan

The idea of object protection is an outcome of the planning process and it decides about quality and proper function of security system. An owner of an object prepares concepts of protection (a plan of critical infrastructure object). A notice from Government Centre for Security stating a "critical infrastructure object" allows to create a plan for it. The structure of such a plan is regulated by the Council of Ministers regulation dated 30 April 2010[29].

According to the regulations this plan is made in paper and electronic version thus it should consist of the following elements: 1) general data: name and location of critical infrastructure, details of a critical infrastructure operator (name, address, the seat and numbers of statistical number - REGON, tax identification number – NIP, company registration number – KRS), data about managing staff in the name of the owner (name, address, the seat and REGON, NIP and KRS), personal information of a person responsible for maintaining contacts with proper entities in the field of CI protection, - personal information of a person drawing up the plan, 2) critical infrastructure data: characteristics and basic

[27] Act on the protection of persons and property Article 2, point 5.

[28] *Ibidem*, Article 2, point 7.

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

technical data, a plan (map) with given object location of installations or system, functional connections between objects, installations, devices or services, 3) characteristics: dangers to critical infrastructure and risk assessment for their occurrence and foreseen scenarios, interdependencies between critical infrastructure systems and estimating the risk of their occurrence and foreseen scenarios, ability to use own resources to protect critical infrastructure, own resources governed by local authorities possible to be used in case of critical infrastructure protection, 4) crucial variants: operating during dangers or interfering with work of critical infrastructure, providing critical infrastructure functionality, rebuilding critical infrastructure, 5) providing cooperation with (depending on location): crisis management centres, public organization bodies[30].

Task analysis

The task analysis is usually understood as a set of team proprietary rules due to understanding the received task and circumstances and conditions for its execution. This process should let understand the aim of implementation of security system in accordance to the role and tasks fulfilled by protected object, understand conditions for realization of object protection and intentions of the ordering protection[31].

During the task analysis it is necessary to consider the following problems:

1) what is the destination of the prepared security system?
2) what are orderer's expectations – what is the aim of created security system?
3) what are the tasks in accordance to the detailed aim dealing with protection?
4) what is necessary data to make a decision about the way for organizing security system?
5) which tasks need to be done and what is the order of their appearance?
6) what timing should be devoted to organise security system?
7) who should be involved in the team proprietary in accordance to foreseen tasks[32]?

[30] Regulation of the Council of Ministers of 30 April 2010 on critical infrastructure protection plans (Journal of Laws No. 83, item 542).

[31] *Ibidem.*

[32] *Ibidem.*

The outcomes of this consideration should be highlighted as conclusions and should allow to make precise general concept of a security system. The outcomes should deal with:

- aim of created security system, especially concerning place or time in which a perpetrator on the object should be detected according to orderer's expectations;
- what is the object of protection by created system?
- what is the priority of security tasks and what elements should include the security system (types of a system, types of signaling)?
- whether there are any limits in creating security systems (due to task analysis and orderer's expectations)?
- what data is needed to make a decision about the shape of the security system to be created?
- what is the time limit to create the security system in the period assigned by the orderer[33]?

General idea for creating the system, which is a derivative of requests from the task analysis, should include general data about the future system and it has not stated as the final solution yet.

a) Object assessment and its surrounding

Another step for action to be planned is object assessment and its surrounding. The consideration should confirm or verify draft assumptions for the conception of created protection. When taking into account a facility the building itself is assessed according to its technical condition, present security and its quality and object's destination. In case of other objects, e.g. being a part of IT systems the assessment includes security systems and conditions in which they are present, especially taking into account any threats that lead to their dysfunction[34].

Before we assess object's technical condition we need to consider the following problems: durability of the construction in accordance to quality of materials used while building; floor plan and communication string (corridors, staircases, escape routes); entrances and drives to the object (number, way of protection, location according to the assessed object and surrounding area); what are object's technical supports and their usefulness; sensitive areas in the object under specific protection (places easy to destroy, rooms with important technical devices or classified documents, managing site, warehouses, communication paths, espe-

[33] Regulation of the Council of Ministers of 30 April 2010 on critical infrastructure protection plans (Journal of Laws No. 83, item 542).

[34] *Ibidem.*

cially lifts). The conclusions concerning the evaluation of protected object should help while verifying prior concept for protection, accepted as the outcome of the task analysis, hence the consideration of these needs to be taken into account: needs for strengthening (or not) the object construction to condition that allows to incorporate foreseen devices and alarm systems: changes (or not) in placing entrances and ways to secure them; defining places of extreme importance and deciding about making changes (or not) in previously approved ways and forms of protection of sensitive part of the building[35], described in preliminary concept.

While assessing a team preparing this conception (and later a plan) of object protection should take into account: object location in comparison to a communication system (drives, available means of transport to use); possible directions and ways of secretive approach to a building; object urban surrounding (distance to other buildings) including important or presenting risk objects and the specification of the object surrounding area; location of forces and rescue units (Police, fire brigades, emergency service, Municipal Guards) Results of object assessment should make the team proprietary sure about correctness of accepted assumptions dealing with object protection or indicate what extra activities need to be undertaken to reach the aim of protection given by the orderer[36].

b) Assessment of possible threats to critical infrastructure objects

According to the created defense conception it is important to take into account the analysis and estimation of threats that may influence the prepared system of protection. When analysing threats it is crucial to consider the following conditions: purpose of the object, its character and significance and threats because of unlawful actions; probable criminal activities or possible timing and place of occurrence of foreseen threats; structure of organised crime on the site, where the object is located; up-to-date number of experienced activities and character of criminal acts present in the object's neighbourhood and probability of their appearance in the protected object; probability of occurrence of other threats; effectiveness of hitherto object protection tasks[37].

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

[36] Regulation of the Council of Ministers of 30 April 2010 on critical infrastructure protection plans (Journal of Laws No. 83, item 542).

[37] *Ibidem.*

When analyzing probable threats because of the object's character and its significance we need to indicate threats against life and health of people working (being) there, property threats, alternative threat against public policy on the area of the object, random threats and other possible threats including forces of nature. The results of the study and assessment of possible object threats should lead to the following hints to be considered: a list of possible object threats and probability of their occurrence; a list of possible perpetrators of specific threats and ways and motifs of their hostile activity; possible directions and entrances to the object; probability of overcoming present (foreseen) security system. The conclusions after the analysis of possible object threats should be used as information which shall make it easy to verify prior concept for protection accepted as the outcome of the task analysis[38].

c) Calculation of forces and means

Another step while creating the concept of defense is defining possible forces and means to be used to neutralize the recognised threats. A wide range of solutions allows to incorporate the following: legal means; organisational-tactical means; architectural-constructing means; mechanical, electronic security and physical security. The support of the police and rescue services should be also taken into consideration. Knowledge about threats is the basis to indicate actions preventing from their occurrence as precautionary activities[39].

When calculating forces and means necessary to create protection system it is needed to justify:

1) what is the indispensable number of security in comparison to the foreseen tasks (are present-day services efficient or not)?
2) where should physical elements of security system be located?
3) where should logistics elements and those providing functionality of physical security if used (guardhouse, weapon and ammunition storage) be located and what are ways to secure them?
4) ways to use technical means of security;
5) ways to manage protection systems (management rooms, their equipment, communication system, alarm system);
6) necessary documentation[40].

[38] Regulation of the Council of Ministers of 30 April 2010 on critical infrastructure protection plans (Journal of Laws No. 83, item 542).

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

[40] *Ibidem*.

Calculation of necessary forces and means is the final element to verify initial assumptions for defense concept. While calculating forces and means necessary for creating a protection system is needed to justify the following:

1) what it the indispensable number of security in comparison to tasks foreseen for it (are present-day services efficient or not)?
2) what tasks should be performed by elements of protection system?
3) where should logistics elements and those providing functionality of physical security if used (guardhouse, weapon and ammunition storage) be located and ways to secure them;
4) sequence of tasks while defining necessary forces and means can be as the following:
5) defining the kind and number of physical elements of object security system,
6) defining tasks of particular elements;
7) calculate number of employees who are necessary to provide functionality of security system;
8) count necessary amount of weapons and ammunition and other indispensable equipment;
9) set number of devices and technical systems supporting objects' security[41].

Equipment, armed physical security forces are regulated by the Act on protection of person and property. Assessment of the situation is the final part for creating the concept of protection. Either the form or the content is not fully formalized but we can take into account the following elements: aim of protective actions, criteria for a security system, significant limits while running the activities, conclusions after object and location assessment, character of threats and the perpetrators, security system, possible changes that need to be done in the object, schedule of tasks while creating security system, charts and sketches as possible enclosures[42].

Approved concept of protection will be helpful while creating critical infrastructure security plan. The legal basis for creating CI plan is information passed by the director of Government Centre for Security to place an object (system) on the list of National Program for Critical Infrastructure Security.

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

[42] Regulation of the Council of Ministers of 30 April 2010 on critical infrastructure protection plans (Journal of Laws No. 83, item 542).

d) Critical infrastructure protection plan

According to the regulations this plan is made in paper and electronic version thus it should consist of the following elements:

1) General data: name and location of critical infrastructure; details of a critical infrastructure operator (name, address, the seat and numbers of statistical number - REGON, tax identification number – NIP, company registration number – KRS); data about managing staff in the name of the owner (name, address, the seat and REGON, NIP and KRS); personal information of a person responsible for maintaining contacts with proper entities in the field of CI protection; personal information of a person drawing up the plan.

2) Critical infrastructure data: characteristics and basic technical data; a plan with given object location of installations or system; functional connections between objects, installations, devices or services.

3) Characteristics: dangers to critical infrastructure and risk assessment for their occurrence and foreseen scenarios; interdependencies between critical infrastructure systems and estimating the risk of their occurrence and foreseen scenarios; ability to use own resources to protect critical infrastructure; own resources governed by local authorities possible to be used in case of critical infrastructure protection.

4) Crucial variants: operating during dangers or interfering with work of critical infrastructure; providing critical infrastructure functionality; rebuilding critical infrastructure.

5) Providing cooperation with (depending on location): crisis management centres; public organization bodies[43].

The plan is signed up by a critical infrastructure organizer. The established plan is consulted with: the voivod, voivod Fire Brigade Commander-in-Chief, voivod Police Commander-in-Chief, director of regional board for water management, voivod on-site inspector, voivod vet, Maritime office director, minister (government authorities manager) responsible for a certain system where critical infrastructure was included[44].

Critical infrastructure protection plan is a classified document. There are many other plans and programmes whose basic rule is devoted to preventing, preparing and reacting to crisis events. Such documents prepared according to legislative papers include plans for object protection and emergency plans. The plans for object protection according to Person and Property Protection Act should consist of the following ele-

[43] *Ibidem*.

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

ments: production specimen or kind of a business, potential danger analysis and present-day level of object security, up-to-date analysis for security level, information about armoured security staff, data for technical security, rules for organising and providing security[45].

The Regulation of the Minister of Economy, Labour and Social Policy is the base for preparing emergency plans, which should include[46]:

1) indicating a list of people authorized to start rescue procedures and those in charge of managing rescue actions and coordinating actions disaster recovery,
2) a list of forces and life-saving appliances and supporting forces that are taken into account when saving and recovery,
3) description of a system used to inform the society about dangers of a running company/business, accepted prevention means and actions to be taken during breakdown
4) procedures for informing people and proper authorities about breakdown danger or its occurrence,
5) procedures for civil evacuation,
6) procedures for medical help to those in need,
7) procedures for actions during tragic breakdown,
8) procedures for after-breakdown actions,
9) setting rules for securing logistics of rescue forces,
10) necessary information depending on kinds of danger and local conditions.

Security of critical infrastructure tends to be treated as national protection. Access to key services tends to be a tangible aspect of national security and country's duty for citizens[47].

Conclusion

When considering country's legislative actions it is rudiment to undergo any actions leading minimize the risk of disturbing CI functions. Providing deed to a property where CI is located allowing for entrance to CI and securing oneself via media contracts are examples of good deeds in this subject area.

[45] *Ibidem*.

[46] Regulation of the Minister of Economy, Labor and Social Policy of 17 July 2003 on the requirements to be met by emergency plans (Journal of Laws No. 131, item 1219, as amended).

[47] *Strategy for the Development of the National Security System on April 2012, section 6*, Ministerstwo Obrony Narodowej, http://www.mon.gov.pl (5.02.2022).

Bibliography

Critical Infrastructure Protection III, eds. Ch. Palmer, S. Shenoi, New York 2009.

Jurgilewicz M., *Rola podmiotów uprawnionych do użycia lub wykorzystania środków przymusu bezpośredniego i broni palnej w ochronie bezpieczeństwa i porządku publicznego*, Siedlce 2017.

Jurgilewicz M., Dana A., *Prywatyzacja bezpieczeństwa i porządku publicznego – specjalistyczne uzbrojone formacje ochronne* [w:] *Państwo. Prawo. Bezpieczeństwo,* tom III, red. A. Babiński, M. Jurgilewicz, N. Malec, Szczytno 2017.

Michalski K., Jurgilewicz M., *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Warszawa 2021.

Pyznor M., *National Programme for Critical Infrastructure Protection – conference materials. Critical Infrastructure Protection – the assessement of the need and abilities*, Szczytno 2010.

Regulation of the Council of Ministers of 30 April 2010 on plans for protection critical infrastructure (Official Journal dated 2010 No 83, position 542).

Rysz S., *Zarządzanie kryzysowe zintegrowane*, Warszawa 2020.

Strategy for the Development of the National Security System on April 2012, section 6, Ministerstwo Obrony Narodowej, http://www.mon.gov.pl

The Act for crisis management dated 26th April (Official Journal 2007 No 89 position 590).

The Act on protection of person and property, (Official Journal 1997, No114 position 740).

The Act on Universal Duty to Defend the Republic of Poland dated on 21st November 1967 (Official Journal 1967 No 44 position 220).

The Council Decision on 2nd February 2007 establishing for 2007-2013 as a part of a general programme – detailed programme dealing with security a protecting people. *Preventing, readiness and managing results of terrorism and other kinds of risk for security*, (Official Journal UET dated on 2007, No 58, position 1)

The Council Directive 2008/114 WE dated on 8th December 2008 (Official Journal EU dated on 2008, No 345, position 75).

The Regulation of the Council of Ministers of 24th June 2003 on the structures especially important for the national security and defence (Official Journal 2003 No 116 position 1090).

Zieliński K., *Ochrona ludności. Zarządzanie kryzysowe*, Warszawa 2021.

Planowanie i organizowanie ochrony infrastruktury krytycznej

Streszczenie

Artykuł poświęcony jest planowaniu i organizacji ochrony infrastruktury krytycznej. Wskazano w nim sposób planowania oraz przedstawiono układ planu ochrony infrastruktury krytycznej. Najważniejszą rzeczą jest ochrona krytycznych elementów infrastruktury, z których obywatele korzystają na co dzień. Mowa więc w artykule o systemach zaopatrzenia w energię, zasobach energetycznych i paliwach, systemie zaopatrzenia w żywność i wodę. A przede wszystkim o systemach finansowych, opiece zdrowotnej i ICT.

Słowa kluczowe: infrastruktura krytyczna, ochrona, system ochrony, plan ochrony