CRITICAL INFRASTRUCTURE PROTECTION

Abstract: Place and role of critical infrastructure in our social life seem to be noticed by politicians and policy-makers even during crisis, because it is seen to be a starter of economical growth. It is hoped that ideas included in 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.

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

Introduction

The term critical infrastructure is a quite young wording, because it was spread out in the 90s of the 20th century. At that time there were many serious cases of blackout in the USA thus they caused many difficulties to millions in inhabitants. Such events are typical for high-tech developed countries with dense energetic network and they are not only devoted to the USA but they are focused on other countries and Poland itself. Blackout in Poland in the surrounding area of Szczecin in winter in 2009 is the example of such actions, because Szczecin agglomeration was not provided with electricity for many days.

1. Legal basis for critical infrastructure protection

The term mentioned previously [1] 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 preventing from terrorist attacks. In 2005 the so called "green book" was accepted, which included political options dealing with preparing a security programme and a system warning about dangers for critical infrastructure system [2]. Another step on the road to minimize 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 Council, consulting current arrangements, indicated that the main responsibility for protection of critical infrastructure belongs to Member States, owners, operators and users [3]. The consequence of further actions was a directive of the European Council specifying rules for recognizing and determining European critical infrastructure [4]. 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. 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 and in the Regulation of the Polish Council of Ministers of June 24th, 2003. The data included in the documents does not respond directly to critical infrastructure, but the analysis of terms used referring to enumerated objects reflects similar meaning.

**B. The European Union documents**

Regulations concerning appointing and critical infrastructure protection were included in either national or European documents. The crucial document that has been recalled previously is the Council Directive 2008/114/WE on the identification and designation of European critical infrastructures and assessment of the need to improve its protection. It also mentions that in the territory of the Community there is a number of critical infrastructures whose disruption or destruction would cause cross-border implications. It concerns cross-sectors resulting from interdependence of connected infrastructures. This type of ECI needs to be recognized and appointed with mutual procedure. Regulations and guidelines included in this Directive were supposed to be incorporated till 12th January, 2011.

**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 (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 functional 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.

**2. Preparation and 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 [5].

**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 [6] and leads to physical security and technical protection. We cannot talk about exhaustion of conditions 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) [7].

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 [8].

Physical protection avoiding access of unauthorised staff is usually divided to 3 sections: external; internal; peripheral.

*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.

**B. Planning protection of critical infrastructure objects**

Protection of critical infrastructure is based on preparing and implementing it. The preparation includes planning and organizing tasks. Planning included 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 Misters regulation dated 30 April 2010.

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;
– interdependies between critical infrastructure systems and estimating the risk of their occurrence and foreseen scenarios;
– 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.

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.

Critical infrastructure protection plan is a classified document.

There are many other plans and programs 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 Persons and Property Protection Act should consist of the following elements:
– production specimen or kind of a business;
– potential danger analysis and present-day level of object security;
– information about armoured security staff;
– data for technical security;
– rules for organising and providing security.

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

a). list of people authorized to start rescue procedures and those in charge of managing rescue actions and coordinating actions disaster recovery,
b). a list of forces and life-saving appliances and supporting forces that are taken into account when saving and recovery,
c). 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,
d). procedures for informing people and proper authorities about breakdown danger or its occurrence,
e). procedures for civil evacuation,
f). procedures for medical help to those in need,
j). procedures for actions during tragic breakdown,
i). procedures for after-breakdown actions,
k). setting rules for securing logistics of rescue forces
l). 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 [9].

Conclusions.
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. We are also talking about how to agree on a protection plan. The most important thing is to protect critical infrastructure components that citizens use on a daily basis. We are
talking about energy supply systems, energy resources and fuels, food and water supply system. And above all about financial systems, healthcare and ICT.

References