SOME PROBLEMS OF CRITICAL INFRASTRUCTURE PROTECTION IN REPUBLIC OF POLAND

Witalis PELLOWSKI *)

ABSTRACT

The paper presents the structure, tasks and competencies of the Polish government and the authorities responsible for security in crisis management system. On examples, the "National Programme for Critical Infrastructure Protection" and the "National Crisis Management Plan" presents a system of mutual cooperation, exchange of information and coordination of ongoing projects.

Key words: critical infrastructure, security, crisis management

ABSTRACT

W artykule przedstawiono strukturę, zadania i kompetencje organów administracji RP oraz instytucji odpowiedzialnych za zapewnienie bezpieczeństwa w systemie zarządzania kryzysowego. Na przykładzie „Narodowego programu ochrony infrastruktury krytycznej" oraz „Krajowego planu zarządzania kryzysowego" zaprezentowano system wzajemnego współdziałania, wymiany informacji i koordynacji realizowanych przedsięwzięć.

Key words: infrastruktura krytyczna, bezpieczeństwo, zarządzanie kryzysowe

1 INTRODUCTION

Dynamically changing security situation forces the creation of effective systems of risk prevention. The object of particular concern government is to ensure the continuity of the basic elements of the systems infrastructure to ensure satisfying the needs of society and the economy.

*) Witalis PELLOWSKI, PhD, The General Tadeusz Kosciuszko Military Academy of Land Forces, Czajkowskiego Street 109, 51-150 Wroclaw, Poland, witalis_pellowski@wp.pl , phone +48 717658361, fax +48 717658425

The result of uncontrollable events caused by forces of nature (natural disasters) or deliberate human activity (anthropogenic factors such as terrorism, regional conflicts etc.) can be damaged or destroyed facilities are important for the efficient functioning of the state and its citizens. Such incidents can have a big impact on economic development and political stability. Particularly important objects - are defined as critical infrastructure (CI) - play a key role in the functioning of the state and the lives of its citizens, and its protection is one of the priorities facing the Polish state.

The Act of 26 April 2007 [1] on emergency management defines critical infrastructure as systems and their constituent functionally interrelated objects, including building structures, equipment, installations, services essential for the safety of the state and its citizens, and to ensure the smooth functioning of the public administration, as well as institutions and enterprises [2].

2 SCOPE, OBJECTIVES, PRIORITIES AND PRINCIPLES OF THE PROGRAMME

Critical infrastructure protection is a vital process involving a large number of areas of competence and task forces and involving many stakeholders. This process includes all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructure also involves gradual achievement of expected results and continuous improvement. Tasks in this area include risk prevention and mitigation, to reduce vulnerability to threats to critical infrastructure and the rapid restoration of its proper operation in the event of any events that might disrupt them.

This document is a concise and comprehensive defines the vision and objectives of the protection of critical infrastructure, the model of cooperation in the tasks, roles of participants and good practice for protecting CI.

National Programme for Critical Infrastructure Protection is based on Article. Paragraph 5b. 1 of the Act on Crisis Management [1]. Operators much of CI are private businesses not related with public administration. The program establishes a framework within which public administration and CI operators cooperate to ensure the continuity of CI, thereby protecting the economic and social foundations of our country. Programme outlines mechanisms for the development of partnerships between public authorities and operators in the protection of CI.

Protection of CI as a gradual process of investigating the expected results and continuous improvement. It is not a state, much less the final product. The program itself is not limited by it no end date. Nevertheless, it is assumed that the program contained in the targets should be reached within six years. Attention to proper adaptation of the implemented solutions that makes program will be updated at least every two years, taking into account the changing environment and the characteristics of the protection of CI.

In order to optimize the proper identification procedures CI Government Security Centre (GSC), in cooperation with the ministers and heads of central agencies and with the support of private entrepreneurs, has developed criteria for identifying CI. Shown numerical values used to characterize the properties, due to which the

infrastructure is classified as CI. In the absence of such a possibility, described the functions performed by the test infrastructure.

Identification of the CI, in accordance with the agreed methodology is divided into three steps below:

First stage - in order to make a first selection of objects, installations, facilities or services that could potentially be considered for CI in the system, the system infrastructure criteria must be applied system-specific CI system;

The second stage - to check whether an object, device, system or service plays a key role in the security of the state and its citizens, and that is to ensure the smooth functioning of the public administration, as well as institutions and entrepreneurs, infrastructure selected in the first stage should be used the definition in art. 3 Section 2 of the Act on Crisis Management [1];

The third stage - in order to assess the potential effects of damage or non-functioning of the CI potential, the infrastructure selected in the first stage and the second przekrojowe1 criteria must be applied, with the potential CI must meet at least two cross-cutting criteria.

CI is meeting the needs of all citizens. The protection cannot therefore be regarded as the exclusive domain of any of the participants in the program. The skills and knowledge of specific IK system to help achieve the objectives of the Programme. Determining competence program participants, understanding the roles and responsibilities of each of them in the protection of critical infrastructure RP is the basis of effectiveness and sustainability undertaken in this respect the effort and contribute to the achievement of the objectives of the Programme. The Program requires the involvement of all possible interested parties, but the main effort lies in accordance with their respective powers, the GSC for Security, ministers and managers of central offices and operators of critical infrastructure in the list of critical infrastructure. CM Act [1] defined the responsibilities of those involved in the protection of CI. Responsibilities of authorities under other provisions of the Act, especially in light of the inclusion of tasks related to the protection of CI in crisis management plans remain unchanged.

Table 1 Shared responsibility for Critical Infrastructure

Critical Infrastructure Systems	**The Minister responsible for the system of critical infrastructure**
The system of energy supply, energy resources and consumption	Minister of Economy Minister of Treasury
The communication system The telecommunication networks	Minister of Administration and Digitization
The financial system	The Minister of Finance
The food supply	Minister of Agriculture and Rural Development
Water supply system	Minister of the Environment Minister of Administration

Critical Infrastructure Systems	The Minister responsible for the system of critical infrastructure
The health care system	Minister of Health
The transport system	Minister of Transport, Construction and Maritime Economy
Rescue System	Minister of the Interior
System to ensure continuity of government	Minister of Administration
The production, storage, handling and use of chemicals and radioactive substances including hazardous pipelines	Minister of the Environment

President of the Republic of Poland, although it is not directly involved in the task for the protection of CI, because of its expertise in the area of national security is an important element of the protection of CI. It is a guarantee of the highest state authorities involved in the process of improving the level of safety CI and thus the state. President takes part in the program in terms of its constitutional competencies including national security and defense. It supports the government and local government in efforts to protect the CI and to achieve the objectives of the Programme.

The Council of Ministers shall exercise executive authority and directs the administration of the government. The tasks of the Council of Ministers on all aspects of political, economic, social and cultural state, including ensuring internal and external security of the state and public order. The Council of Ministers, a resolution adopting the National Programme for Critical Infrastructure Protection, gives impetus to achieving the objectives pursued by the subordinate authorities and bodies.

Voivodes play an important role in the protection of critical infrastructure and disaster management. In accordance with regulatory requirements, the task of Governors and the appropriate organizational units for crisis management in the regional office. Provincial level is the point of transition between the system and the recognition of territorial responsibilities for the protection of critical infrastructure and services, subject to the guards and inspections.

The specific role has been assigned to the Internal Security Agency (ISA). Head of the ISA in the event that the information about the possibility of a crisis which is the result of a terrorist event, threatening the critical infrastructure, human life or health, property of considerable value, national heritage or the environment, may make recommendations to the authorities and entities at risk of these activities and providing them with the necessary information to address threats. Head of the ISA supports public authorities in the activities related to the prevention, prevention and removal of the effects of terrorist events.

District governors, mayors and presidents of cities and their subordinate services play an important role in protecting the population exposed to the potential consequences of failure in the CI and the protection of CI, allowing direct and fastest direct support.

3 CRITICAL INFRASTRUCTURE PROTECTION

The protection of critical infrastructure consists of the following steps:

1. An indication of the scope, objectives to be achieved in the framework of the protection of CI and the public of these activities;
2. Identification of critical resources, functions and determine networks (dependencies) with other CI systems, including operators and authorities;
3. Defining the roles and responsibilities involved in the protection of CI;
4. Risk assessment and identify priorities for action and to prioritize them based on the results of risk assessment;
5. The development and implementation of the system of critical infrastructure protection, including the development and approval of plans to protect and restore CI;
6. Testing (through exercise) and review (through audit and self-esteem) CI protection system and to measure progress towards achieving the goal;
7. Improvement, defined as the introduction of modifications and adjustments as a result of testing, inspection and measurement.

The need for continuous improvement in the recognition process allows the protection of CI Deming cycle [3, 4]. Treatment process in CI protection cycle allows, after the measurement results, to take corrective action or improvement to the stage where it was found a deviation from the expected results. It is also possible to redefine the goals. Another repeat the cycle should bring us closer to achieving them. Deming cycle is applied at each level, which is the protection of CI and should be repeated at fixed intervals.

Measures for the protection of CI are financed from its own funds and program participants planned their budgets:

- For administration pursuant to Art. 26, paragraph 1 and paragraph. 2 of the Law on crisis management [1];
- For operators CI on the basis of Art. 6 of the Law on Crisis Management [1].

GSC in collaboration with the ministers responsible for CI systems, will seek to prepare and submit for approval by the Minister of Science and Higher Education by the Steering Committee of the National Research and Development Project of the strategic program for research and development to increase the security in the framework of CI research or development for national defense and security.

CONCLUSIONS

The expected result of the implementation of the Programme will achieve the strategic aims and operational objectives. However, given that these effects occur in the longer term, closer to the effects of the Programme will include:

- Raise awareness of the critical infrastructure, its importance for national security threats, which may be subject to and protect against these risks;
- The final formation, based on the experiences, roles and responsibilities in the protection of CI and introduce a mechanism of coordination;
- Assess the risk of disruption of the functioning of CI, from all types of threats;

- Establish a hierarchy of priorities playback CI;
- Development of the operators CI acceptable level of risk and the expected disruption of CI, which remains in their possession;
- Detect unacceptable risk areas and take corrective action;
- Improving the information flow between the operators CI, and public administration;
- Determining the scope operator CI support public administration in emergency situations;
- The introduction of the legal acts necessary changes to facilitate the protection and restoration of CI;
- Start work on generating and publishing best practices in the field of CI;
- Start work on standardization of forms and principles of protection of CI.

To examine the effectiveness of the system of protection of CI will be implemented in the future by the major operators, with the support of the public administration as substantive audit procedures. The reports of the audits will be forwarded to the Minister responsible for the CI system.

Verification of the system of cooperation between participants CI protection will be implemented in the form of practical exercises involving emergency services and safety (police, fire brigade, ambulance). Pending the development of a comprehensive and measurable indicators showing the effectiveness of the CIP will be prepared reports showing the following numbers (parameters):

- CI operators in the designated contact person in charge of the administration;
- Subjects with approved security plan;
- Operators using internal controls and security audit CI;
- Exercises broken down by CI systems compared to previous years;
- Active participants in the forums, and web-based platform.

Reports will be made based on surveys of safety facilities, equipment, systems and services CI, internal audit reports submitted by the operators of CI and conclusions of the exercises provided by entities exercising.

REFERENCES

[1] Crises Management Act dated. 26.04.2007., Journal of Laws of 2007, No. 89, poz.590. and the Law amending the Law on Crisis Management, Official Journal of 19 August 2009.
[2] Collective publication, National Programme for Critical Infrastructure Protection, RCB Warszawa 2013
[3] HAMROL, A., MANTURA W: Zarządzanie jakością. Teoria i praktyka. WNT: Warszawa 2003. 67 s. In.:
[4] ZAMIAR, Z., ZAMIAR, A., Zarys teorii zarządzania kryzysowego, MSLiT, Wrocław 2010.

Článok recenzovali dvaja nezávislí recenzenti