IMPORTANT EXPERIENCES OF CIP FROM THE PERSPECTIVE OF A FIGHT AGAINST TERRORISM – MALICIOUS ATTACKS

Ján Buzalka, Prof.

jan.buzalka@minv.sk

Police Academy in Bratislava, Slovakia

Abstract

The problematic aspects of critical infrastructure in an integrated frame in Slovakia are recently not codified in any legal norms. The law does not stipulate competences or responsibilities towards any state administration institution, nor the advisory governmental body within the Slovak Republic. Self-governing regions, cities, municipalities and legal persons do not have established their share for the fulfillment of tasks in the respective area, either. The topicality of the need to legislatively adjust competences and responsibilities of public administration bodies and also the private sphere (juristic and natural persons) grows.

Within the context of critical infrastructure and its interconnection into the European space in the first few years of the new millennium, the **international cooperation** started to be developed and intensified not only in the standard areas of defense and protection of critical infrastructure in political and military sphere, but also in the area of science and research, critical infrastructure personnel education, as well as in particular specific areas. We can mention the European Program for Critical Infrastructure Protection (EPCIP) as an example of recent significant eventuation of these processes of the cooperation. Mission of the aforementioned program is to assist the existence of standard and uniform level of defense and critical infrastructure protection within the entire European Union, in order to create an equal level of defense and protection for all levels of critical infrastructure, and the minimal number of real, as well as potential points of failure and fast correction measures to exist and to be prepared and tested. Attention began to be paid also to questions of sensitivity and resistance of critical infrastructure sectors. These requirements started to have exact contours in the

fundamental demarcation for the expert community, where they are understood as following: **Resistance of critical infrastructure** is the ability to face random, as well as intentionally undesired – generally negative action upon its individual parts in substantial, even marginal intensity. **Sensitivity of critical infrastructure** is the feature, that expresses the capability of the system to register negative activity, or processes, directed at the core of the given system itself and activate the adequate defense and protective mechanisms for the preservation of its stability and functionality.

The EU requirement to identify subjects of European critical infrastructure, subjects of national and local critical infrastructure on the territory of each member country stems from the premise that the level of protection should not be the same for all critical infrastructures, but it should be derived from the impact.

Presented approaches generalized the fact that a terrorist attack or military action is, in a significant scope, focused on those parts of society, that if destroyed or damaged, lower the defense capacity of the state or coalition. Aims of antagonist‘s aggression are generally the elements of the critical infrastructure of the state and region. Critical infrastructure is composed of facilities, services and information systems, that are vital for the population and for the management of the state, and destruction or dysfunction of which may endanger the security interests of the state. Especially these present the objects of significant importance, other important objects, selected information and communication instruments as well as facilities for the production and supply of water, electricity, petroleum and natural gas and other parts of economy and society designated by the government or other competent institution of state administration, that are inevitable for handling critical situations, protection of population and property, for ensuring the minimal course of economy and state management, as well as its external and internal security, being therefore needed to be specifically defended and protected.

Critical infrastructure and its identification

Methods of risk analysis, risk modeling and other methods were utilized as the foundation for identification of the critical infrastructure on individual levels (European, state, local) (Buzalka, 2005: 66-76). Defined general character of identification of the critical infrastructure stems from the requirement that criteria have to be applied in a sectional way in all sectors of critical infrastructure, with the primary regard to the seriousness of the influence of violation or destruction of particular infrastructure, its sector, sub-sector or its element, which is important for some of the areas of security of the society, state, region. As the general criteria of critical infrastructure the following are generally considered:

- volume of consequences and the potential to cause losses of lives, to act negatively upon the welfare of population;

- economical effects (economical impact) with the emphasis on seriousness of economical losses or worsening of production or services;
- impact upon the public with the emphasis on the number of affected citizens, including the impact upon the confidence of population in the ability to solve the critical situation in a competent and effective way;
- effects on environment and life conditions of people, domestic animals and reasonable life conditions for existence;
- in case of infrastructure also to regard accessibility of alternative reserves, including duration of violation and renovation of services;
- probability that the element may be the target of a terrorist or military attack, as well as the fact that it may be threatened by other risk factors from the viewpoint of possible influence or prosperity of the state, as well as the welfare of population, movement of large number of people, easy accessibility, etc.;
- consequences of attack or influence of other risk factors upon the element of critical infrastructure will cause the threat or violation of political course of the state or its defensive ability;
- by its structure, function, material or virtual base, the element of the infrastructure in the system of protection and defense of society is unique and irreplaceable;
- territorial impact of negative consequences – several EU countries, state, local state level;
- time consequence – duration of consequence = short termed, middle termed, long termed, etc.;

In a simplified way, the conclusion can be made that the decisive criterion for determination of the elements of critical infrastructure is the unacceptable risk in the plane of community, state and local level (Buzalka, 2005: 50-53).

Critical infrastructure can be understood as a complex of physical or virtual systems, institutions, facilities and other services, destruction, insufficiency or violation of which could cause the violation of societal stability and security of the state, it could evoke the critical situation or it could seriously influence the functioning of the **state administration and self-administration** in critical situations.

Violation or collapse of critical infrastructure can endanger the very production of food-stuffs, heating, industrial production and it can, in fact, violate and disrupt the course of society. As a result, the attack against any element of critical infrastructure may result in malfunction of infrastructures of regional scope that is also in broader geographical space, which is

mutually interconnected by various nets (physical, virtual or logical connection into nets creates the so-called knots, violation of which leads to regional, whole-state, but also cross-border negative impact). If the guarantee of fundamental state functions fails, we will re-awake their importance and we will want to know the reason why it is so and why the responsible institutions have prevented this disaster.

Violation of key objects of critical infrastructure because of a **terrorist attack**, eventually because of other reasons, such as a big natural or **technological catastrophe** on our territory, would always mean great losses of lives and property (nuclear power plant, reservoir), moral damages (objects with significant symbolic value, memorials) or would lead to disorganization of the society as a whole (seats of central institutions, damage of the sanitary resorts net, sewage tanks, supply net, etc.).

Infrastructure in the Slovak Republic is highly vulnerable, mutually and externally greatly interconnected, however, inevitable for the course of society of the 21st century. Terrorists proved that they are capable to organize attacks in different places at a time. The use of weapons of mass destruction (WMD) can not be excluded. Terrorists plan their attacks in the long term, they inspect the target even several years ahead, they consider all the factors in order to "minimize their own effort and maximize the profit".

In the course of military action or terrorist attacks the attention of the opponent is to a large extent focused on those parts of society, destruction or damage of which decreases the defense capacity of the state and coalition. Aims of the opponent's aggression are generally the elements of critical infrastructure of the state and region. **Critical infrastructure is composed of facilities, services and information systems vital for the population and state management, dysfunction or destruction of which may endanger the state security interests.** These count especially the objects of significant importance, other important objects, selected information and communication instruments, facilities for the production and water, electricity, petroleum and natural gas supply and the other parts of economy and society designated by the government or other competent institution of state administration, that are inevitable for handling critical situations, protection of population and property, for ensuring the minimal course of economy and state management, as well as its external and internal security, therefore being needed to be specifically defended and protected.

Critical infrastructure – facility, system or its parts, material, as well as virtual, that are key for the security of the country and its citizens, for securing proper functioning of state and self-administrative institutions, as well as entrepreneurial and private sector. They are relatively independent

systems, destruction or violation (that is limitation) of which would have serious consequences for the economical and societal stability, defensive ability and the state security, state functioning and preservation of societal functions, it would endanger lives, health, safety and protection of population, as well as quality of life of citizens from the economical and social viewpoint.

Among basic instruments of the system of defense and protection of critical infrastructure we can incorporate:

- instruments for the prevention against threat – legal norms and technical requirements, system of security assurance and security documentation, regime measures of the element, system of warning and notifying the institutions and population, autonomy of the element, etc.;
- instruments for decreasing risks of threat of existence and stability of the element – technical instruments of protection, physical protection and defense, plans of protection and defense, intelligence activity, activity of public administration including prosecution and courts;
- instruments for adverting the attack against the element or system of its protection and defense – intervention of security service, intervention of armed safety corps, intervention of armed forces, intervention of armed forces of allies, etc.;
- instruments for clearance the attack consequences – utilization of reserve machines, interconnection of functioning systems, renovation or substitution of damaged elements, application of directive instruments of state power, creation of the plan of welfare response to weapons of mass destruction (WMD), etc.

According to "CI conception in the SR**",** the sector of national infrastructure is such a sector where the failure (reversible or irreversible) of some of its important functions or some of its elements, predominantly as a consequence of a terrorist attack, causes the threat or violation of some of the state security areas, e.g. the political course of the state including the functioning of public administration, state defense, course of state economy, etc.

Vulnerability of critical infrastructure is a feature reflecting the **weak part of its sector or element**, decreased resistance against possible violation of its functioning, damage or destruction.

"Public order and inside security Sector"

For the need of realization of critical infrastructure defense and protection measures in this sector we can classify the safety threats of the critical infrastructure according to the way and possibility of elimination that is

according to the inevitable reaction of the state. Therefore, the readiness and ability to solve the threat of critical infrastructure is also oriented towards activating individual constituents of protection and defense.

"Emergency constituents Sub-sector"

The following may be integrated into the sub-sector of emergency constituents:

- civil protection of population,
- Fire and Emergency Brigade
- Police Forces.

In the filed of **civil protection** it is needed to transfer the tasks, resulting from identification and protection of elements of power critical infrastructure, into relevant documents. It counts predominantly the elaboration of data into **analyses of possible threat for territory by exceptional events and plans of protection of population, eventually the plans of evacuation and hiding.**

Protection of critical infrastructure is, in a broader view, also the protection against terrorism, **which is the first political priority of the European Union and NATO.** The system of critical infrastructure protection has to be compatible with other countries, especially the EU members, in order to be sufficiently effective[1].

Constantly deepening net character of the infrastructure moves the problematic of critical infrastructure – that is its demarcation, determination of measures of its protection – across the frontiers of one country. Despite national specifications the defined areas of critical infrastructure of individual countries differ very little. (Comparison of sectors included into critical infrastructure in selected countries is shown in the chart in appendix N...) (Seidl, Tomek, 2008: 42).

Within the entire European Union (EU), the most significant documents enabling to fight terrorism actively are European Convention on the Suppression of Terrorism and Declaration on the Fight Against Terrorism. By means of adopting the mentioned documents, conditions for the acceptance the revised **Action Plan of the Fight Against Terrorism** were created – as the fundamental and one of the most important internal documents of the Slovak Republic, that was based on:

- strategic aims of the fight against terrorism,
- deepening of international consensus and strengthening the joint effort,
- limitation of the access to financial and economical sources for terrorists,

[1] Národný program pre ochranu a obranu kritickej infraštruktúry v SR (National Program for the Protection and Defense of Critical Infrastructure in SR).

- prevention of terrorist attacks,
- clearance of eventual attacks consequences,
- compensation to the victims of terrorist attacks
- improvement of cooperation with the third countries in the area of the fight against terrorism.

Key subjects of the fight against terrorism in the Slovak Republic according to the Action Plan of the Fight Against Terrorism:

- intelligence area – prevention of terrorist and risk activities;
- preventive and repressive area – activity of the Police Force specialized units and law enforcement bodies in the area of the fight against terrorism;
- foreign peace and humanitarian area;
- foreign-political area;
- other subjects participating in the fight against terrorism;
- area of coordination, cooperation and interoperation of intelligence services of the Police Force, Railway Police, Bureau of Customs of the Slovak Republic and Armed Forces of the Slovak Republic in the fight against terrorism;
- specific areas in the fight against terrorism.

National concept of the defense and protection of critical infrastructure covers especially the areas: management of the defense and protection of critical infrastructure; determination operation of the state administration institutions in the area of management of the defense and protection of critical infrastructure; demarcation of responsibilities to the operators of critical infrastructure elements; elaboration and fulfillment of safety plans of the operator of a critical infrastructure element, organization and performance of the system of defense and protection of critical infrastructure elements, support of realities, that contribute to the development of defense and protection of critical infrastructure and minimizing potential points and areas of failure, protection of clandestine facts in the field of critical infrastructure.

Area of the management of critical infrastructure defense and protection includes predominantly the tasks and measures such as – performance of risk analyses with respect to the development and parallel changes of security appeals and threats and vulnerable spots of individual elements of critical infrastructure, their possible negative influence on preservation of core functions of the society, security, lives, welfare and life standard from the security, economical and social viewpoint as well as identification of important facilities, premises, information systems within the element of critical infrastructure; demarcation of priorities of counter-measures and optimization of approaches for the defense and protection of critical infrastructure.

Area of the operation of state administration bodies in the field of protection and defense of critical infrastructure – is defined by the law and includes ministries, other central state administration institutions, which have the responsibility for the assigned sector or element of critical infrastructure. During the fulfillment of tasks of the defense and protection of critical infrastructure and their control, ministries cooperate with the state institutions, juristic and natural persons, which are operators of elements of critical infrastructure. Ministries – Ministry of Interior of the Slovak Republic and Ministry of Defense of the Slovak Republic especially: elaborate the concept of defense and protection of critical infrastructure; manage the performance of state administration in this area within the scope of their competence; issue generally binding regulations for the fulfillment of tasks in this area; provide fulfillment of obligatory acts of the EU and NATO in this area; perform and coordinate the control activity in this area; guard the exchange of information in this area in compliance with international agreements; bring forward proposals on the insertion and deleting of element from or into the sector of critical infrastructure to the Government; manage the central evidence of elements of critical infrastructure of all the sectors. Ministries work out the risk analysis of the vulnerability as per the particular sector, elaborate proposals on the insertion and deleting of element from or into the sector of critical infrastructure and forward it to the minister; manage the evidence of elements for the particular sector of critical infrastructure, control fulfillment of tasks of the defense and protection of critical infrastructure, cooperate in the fulfillment of tasks of the defense and protection of critical infrastructure with the bodies performing the tasks in the given sector of critical infrastructure, present the overall report on controls of elements of the sector of critical infrastructure in the regular year. District office in the residence of the region and district office include, the analysis of the territory and plan of protection of the population, consequences of violation of elements of the critical infrastructure and measures for the effective defense and protection of elements of the critical infrastructure; participation in the performance of control activity in this area.

Area of demarcation of responsibilities to operators of critical infrastructure elements determines the responsibilities of an operator to accept all the necessary measures, needed for the protection and defense of the element of critical infrastructure, with the aim to avert, reduce and neutralize the threat and risk of its violation. Operator predominantly: chooses the best accessible instruments of protection and safety of the element of critical infrastructure during the process of construction of new or modernization

of existing facilities; works out and keeps the prescribed documentation and evidence; performs necessary measures for the support of defense and protection of the element of critical infrastructure; assures regular control; provides the relevant institutions the needed interoperation, information and documentation; elaborates the safety plan within the period of three months since receiving the notification, by means of which the element has been assign as the element of critical infrastructure; assures regular practice of critical situations according to the safety plan; advances according to the safety plan in case of violation of the element or immediate threat of violation of the element of critical infrastructure; is capable to prove the fulfillment of tasks determined by the law.

Area of processing the safety plans, organizing and performance of the system for the support of defense and protection on the side of operator of the element of critical infrastructure. Safety plan has been worked out in cooperation with respective institutions and subjects, which are counted on in the interoperation when overcoming threats of violation of the element of critical infrastructure. In the safety plan, the operator identifies facilities of the critical infrastructure and determines security solutions, that exist or will be implemented for the purposes of their protection. Safety plan of the operator includes predominantly: identification of important facilities; individual facility risk analysis and possible consequences with respect to potential threats; determination of main permanent safety measures. Permanent safety measures are those, that specify investments and instruments needed for the security of protection of critical infrastructure. Here we insert especially: technical measures (system of access controls, monitoring and detection systems, protective and preventive instruments); organizational measures and crisis management; measures from the viewpoint of expert preparation of subjects providing the protection of the element of critical infrastructure; specific measures towards safety of information systems.

Area of support of the facts, that contribute to the development of defense and protection of critical infrastructure and minimizing potential points and areas of failure, requires – to build and systematically develop consistent and cooperative partnership among owners, operators and state and self-governing bodies; support the cooperation of individual systems and sub-systems, create reserve or substitution elements of the system of critical infrastructure; realize different defense and protective measure, proportional to the level of potential danger; plan and prepare the tested correctional measures.

From the viewpoint of solving the given content questions, the problematic of recent tasks and measures in the area of defense and protection of critical infrastructure is significant. Among the actual tasks we can integrate:

- to generalize and in practice realize the positive, as well as negative experiences of the companies, organizations, institutions, that differ from the "regular" ones in a way, that they operate under a constant pressure of possible threat and keep the balance between reliability and maximal production;
- to realize security preparation of the defense and protection of critical infrastructure, also for low probable risk with a great impact or disastrous consequence in advance and to solve the future problems today;
- within the context of reality expressing the interconnection and attachment of individual critical infrastructures to solve their defense and protection in a coordinated, systemic and complex way and to respect their individual levels (European, state and local) and interconnection;
- to focus the activities of scientific community and universities upon the solving of selected theoretical and practical questions of the defense and protection of critical infrastructure;
- to assure a continuous preparation and education of owners, managers, employees, etc. of critical infrastructure for flexible reaction, expert improvisation, application of practical skills, etc.;
- to improve information system, monitoring of the stage and performance of elements of the critical infrastructure, quick exchange of information and optimal system of warning and notifying on individual levels.

From the point of view of regional requirements to the defense and protection of critical infrastructure, the attention is oriented especially on the area of protection of elements and sub-sectors of critical infrastructure and support of defense of these parts of the system of critical infrastructure of our state, with the full respect of accessible own powers and sources, as well as real possibilities of allies. Local state administration bodies are responsible for providing the defense and protection of critical infrastructure, e.g.: into "Analysis of the territory from the viewpoint of possible emergency events" will include also the impacts of element violation, that is the elements of critical infrastructure; the tasks and measures for an effective protection of elements of critical infrastructure will be included into the plan of protection of the population; they perform the control of protection of elements of the critical infrastructure; they participate on the preparation

of the territory for the defense also from the angle of problematic of defense and protection of critical infrastructure.

Upcoming period is characterized by growth of complexity and mutual interconnection of individual infrastructures especially in the developed countries and international communities. Complexity and interconnection of infrastructures is a global irreversible tendency, which is, to a significant extent, also the bearer of scientific and technical development, growth of prosperity and welfare, as well as the areas, that may easily become the source of tension or conflict between the states, coalitions, political parties, nations, ideologies, etc. It is exactly the tendency of growth of the infrastructure significance in local, state, coalition, continental and worldwide measure for prosperity, high life standard, and development of humanistic and democratic heritage in all parts of the world, which leads to momentous dependency of these social communities for their optimal and harmonic functioning. Level of dependency of companies on created infrastructures, on the one hand, and the tendency of systemic interconnection of individual infrastructures and their levels with the real tendencies of their failure, damage or threatening, becomes on the other hand a challenge for solving the questions of their security. Experiences from the last years, especially from the terrorist attacks in various countries worldwide, proved that many modern practices of infrastructure protection are ineffective and its is needed to adopt such measures on individual levels, that minimize possible consequences of the events or activities restraining or eliminating individual or whole infrastructures, or their sectors, sub-sectors or elements.

For solving the aforementioned, the fundamental initial solutions were adopted, for example: determination of sectors, sub-sectors and elements of critical infrastructure on individual levels with the acceptance of recommendations of SCEPC of NATO for civil emergency planning; public administration together with the private sphere will be included into defense and protection of selected elements of critical infrastructure with the decisive responsibility of the state; system of the defense and protection of critical infrastructure has to be compatible in NATO and EU countries; principles of subsidiary, proportionality (adequate proportion of components), complementarity (mutual complementation) and mutual dialogue will be asserted; activities and responsibility for the defense and protection of critical infrastructure is divided into individual levels – coalition (NATO, EU), state and local; defense and protection is executed differently by means of powers and instruments of the coalition, state and local level; system of defense and protection of critical infrastructure will dispose of modern operating system at all levels and areas (sectors, sub-sectors, elements); strengthening of research and educational activity in the area of defense and

protection of critical infrastructure will occur, as well as improvement of preparation of participants.

References

1. Buzalka, J. (2005), Všeobecné otázky krízového manažmentu. APZ, Bratislava.
2. Seidl, M., Tomek, M. (2008), Niektoré problémy kritickej infraštruktúry, Civilná ochrana, Vol. 10, No. 6.