ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 31

4th International Conference on Management Science and Management Innovation (MSMI 2017)

Terrorist Threats for the Critical Infrastructure of the State

Bogdan Grenda
Faculty of Finance and Banking
WSB University in Poznan
Poznan, Poland
e-mail: bogdan.grenda@wsb.poznan.pl

Edyta Ślachcińska
Faculty of Finance and Banking
WSB University in Poznan
Poznan, Poland
e-mail: edyta.slachcinska@wsb.poznan.pl

Paweł Majdan
Faculty of National Security
War Studies University
Warsaw, Poland
e-mail: p.majdan@akademia.mil.pl

***Abstract*—Critical infrastructure has a crucial role in the functioning of the state and the lives of citizens by providing social or economic conditions for development and security. Therefore, it can be assumed, that the state for its smooth develop needs solutions which can guarantee the necessary level of protection which are essential to objects being included in a critical infrastructure of the state. This article assesses elements of the critical infrastructure of the state were as well as identified the most probable threats of terrorist attacks. In conclusion introduced the Critical Infrastructure Protection System to counteract terrorist threats.**

Keywords-critical infrastructure; terrorist threats; protection

I. INTRODUCTION

Critical infrastructure is the systems needed to provide a minimum for the functioning of the economy and of the state, which must be preserved in order to provide broadly understood security and key services in the state. Their distortions can occur as a result of unexpected events, caused by the forces of nature or by man. In this respect, it should be emphasized that the presented research results are focused on human activities that endanger critical infrastructure facilities by using different means and methods of terrorist activitiesTerrorist attacks can contribute to disrupting the functioning of the state, its economy and threatening the security of citizens and their property. Thus protecting such critical infrastructure is essential and should be seen in the priority of each state. Ensuring its functionality, preventing threats, determined and effective actions in case of terrorist attacks, integration of not only domestic, but also international action is their main purposes. In this regard, it can be reasonably assumed that the protection of critical infrastructure from terrorist threats is a significant problem due to its complexity, which results from the multiplicity of terrorist threats.

Critical infrastructure protection should be understood as a set of activities that prevent the underhanded getting around on its territory, or external interference which main aim is destruction of personnel or facilities. The purpose of protection is to ensure order and security in the area of the object, counteracting acts of terrorism. Protective measures are to ensure the effective, direct and indirect protection of certain facilities and personnel, which may be the subject of the identification and assault of terrorist groups.

Therefore, the critical infrastructure protection system should protect objects against any external threats and consist in formulating appropriate organizational structures, developing operational procedures, equipping facilities with technical protection measures, etc. The critical infrastructure protection system must be continually improved as new threats are appearing and the potential opponent has increasingly better means of attack. Consequently, the purpose of the article is to diagnose terrorist threats to critical infrastructure and to attempt to formulate assumptions for the creation of a system for the protection of objects in its composition.

II. CHARACTERISTTCS OF THE CRITICAL INFRASTRUCTURE OF THE STATE

The concept of "critical infrastructure" is as old as the old civilization on earth. In ancient Rome, the critical infrastructure was mainly roads and aqueducts. The roads were military in that they allowed for very fast transport of soldiers and military equipment into the threatened provinces of the Roman Empire. Aqueduces, in turn, provided fresh water to the population, which was not only a very innovative technological solution, but also a health and sanitation solution. In ancient China, the critical infrastructure was a wall that provided protection against invaders and facilitated economic, military and cultural development. Critical infrastructure in colonial Spain can be termed gold mines in South America, ports and the fleet that transported this valuable raw material to the country. Today the notion of critical infrastructure is much broader due to technological progress, the emergence of new phenomena, etc. Many critical infrastructure systems, however, remain unchanged to this day.

Critical infrastructure includes energy and fuel supply systems, interconnectivity and teleinformation, and

communication networks, financial, food and water supply, health, transport and communications, rescue, ensuring the continuity of public administration, production, storage, storage and use of chemicals and radioactive substances, including pipelines of hazardous substances [1]. In analyzing critical infrastructure issues, it is important to be aware that it covers systems crucial to the security of the state and its citizens. These include communication, energy and fuel supplies, health care, transport, food and water supplies. Therefore, it can be concluded that critical infrastructure has systemic nature. The system, in general terms, means *the set of interconnected elements, having a defined structure and constituting an ordered whole* [2]. This is important due to the fact that with a systemic approach, it is possible to identify and evaluate the possible consequences of damage or elimination of individual system components with respect to the functioning of the whole. The prerequisite for obtaining reliable research in this field is the prior definition of hazards, which in turn, will make it possible to seek effective alternatives to address the identified risks. In addition, it should be emphasized that with the critical system approach to critical infrastructure, we will be dealing with highly distinctive and highly addicted members [3]. In this regard, it can be concluded that the particular components of the whole will be objects of particular importance, from the efficiency of operation, which will depend on the success of the operation of a particular subsystem. Their destruction or damage will cause distortions for longer periods of time, which could significantly affect social or economic security and the ability to provide national defense and security. Their distortions can occur as a result of unexpected events caused by forces of nature or by intentional or unintended human actions.

III. THREATENING WITH THE TERRORISM TO THE CRITICAL INFRASTRUCTURE OF THE STATE

The concept of terrorism originates from the Latin word *terror* which means *terrible word*, *terrible news* and derivative of Latin verb *terreo* which means to cause horror. Based on the etymological origin of the word it is possible to determine the terrorism as arousing fear and danger. To underline a fact that the encyclopedic definition brightly determines the occurrence of the terrorism, his assumptions and purposes are included.

However, there are many other definitions that aptly characterize this phenomenon, and therefore can be defined as "violence - or equally important - the threat of violence aimed at achieving or serving political ends" [4]. Using violence against individual units or groups of people" [5] or "the use or threat of political, religious or ideological use, violent action against persons, property" [6].

The characteristic of modern terrorism is that "terrorists do not recognize borders, their territory may be any country, often not directly linked to the purpose of the organization's demands. He fights in and out of town. The principle is one-the more spectacular action, the greater publicity and the better effect" [7].

Although the different definitions of terrorism differ from each other, however, as emphasized Walter Laquer, most experts agree that terrorism means the use or threat of violence, a fighting method or a strategy for achieving certain goals; That his aim is to intimidate the state through victims. That it is ruthless and incompatible with humanitarian standards and that publicity is an important component of terrorist strategy [8].

A terrorist attack constitutes a threat of utmost importance to the security of the state. According to previous cases of terrorist attacks, the targets of attacks may be the centers of power, economic and public infrastructure, as well as objects whose destruction represents a serious threat to security, mainly such as: military facilities and civilian government facilities, international airports, large cities and objects of great importance. Terrorists can also conduct attacks on large gathering places, such as sports matches, music concerts, etc., water and food supply systems, utility centers, and shopping centers and enterprise management.

One of the most important features of modern terrorism is its unpredictability as to the place and form of attack, the used means, and the effects it can cause. Terrorists may carry out maslaughters, kidnap people and vehicles including cars and planes. In addition, terrorists are capable of inducing fear by sending explosives or chemicals and biologicals via mail. Thus, each of the systems classified as critical infrastructure may be a potential target for a terrorist attack, although the purpose of the attack may be different. Therefore, threats from terrorist organizations should be considered in relation to systems and their critical infrastructure.

System of the energy supply, fuels and fuels are one of essential systems of the critical infrastructure, which consist of subsystem: productions (of recruiting) of the energy, the transfer of the energy and fuels and distribution of both energy supplies and fuels to recipients. With reference to this subsystem, a direct terrorist attack on the system is possible. Its aim may be the physical infrastructure of the system and attack by a power system in which some power system installations might be used to attack other components of its infrastructure, which may be triggered by a strong electromagnetic pulse in the network to damage computers and telecommunications infrastructure.

Communication systems and teleinformatic networks are systems and networks whose malfunctioning or defect, independent of cause and scope, could pose a serious threat to human life or health, the defense interests and the security of the state and citizens, or expose those interests to at least substantial harm. It results from the fact that it is about daily proper functioning of such systems as: energy, finance, water supply, transport, health care, but also emergency (crisis). A terrorist attack may be carried out in the form of suicide bomb attacks or organized sabotage actions, such as using vehicles designed to destroy the infrastructure and cause staff losses.

Another potential target for terrorist attacks is the state financial system. The facilities in this risk group include the head offices of banks and their outlets, financial institutions,

mints and Security Printing Works, payment systems, accounting centres for payment cards and the cash-machine network. The terrorist attack can assume the form of a bomb attack which aim is destroying the infrastructure and causing of losses in the staff and the clientele or the form of the cyberattack on financial computer systems.

The provision of society in food is an elementary existential necessity. Disturbances in this respect may not only result in social dissatisfaction, but may also cause serious illness and even epidemics. The purpose of terrorist activities in relation to this sector of the economy can be to cause significant human losses, trigger panic, or cause economic loss by halting exports because of food contamination at one of its levels of production. Measures that may be used by terrorists in this activity include particularly biological, chemical or radioactive measures.

No less sensitive system is the water supply system, especially of large urban agglomerations. It consists on outlets of drinking water and water supply. The attack on this system may involve contamination of water intakes by biological or chemical means. The purpose of a terrorist attack involving such weapons would be to cause a large area of death or disease that could take the size of an epidemic, which could result in loss of confidence in the authorities and destabilization of social and political structures.

The health care system is an extremely important system of critical infrastructure that directly affects citizens' sense of security. Attack on objects may be done using chemicals (not necessarily poisonous), or the threat of planting an explosive device that makes the hospital staff to evacuate the sick, involve the rescue and law enforcement. Such actions may constitute an element of diverting the attention of these services from the terrorist attack in another facility or hinder the provision of assistance to the victims of another attack.

An analysis of terrorist attacks carried out in recent years indicates that transport and communication critical infrastructure is one of the main targets of terrorist attacks. All types of transport and communication are covered: air, rail, road and sea and related infrastructure. Therefore, the object of the terrorist attack can be the elements of airport infrastructure and aircraft both in airports and during take-off and landing operations, as well as in flight. They can also abduct a civilian aircraft and then use it to commit suicide on the selected object.

The purpose of the terrorist attack on the infrastructure of the rescue system (Crisis Management Centers, Fire Brigades, Medical Rescue Services, Technical Assistance) will destabilize the management and rescue centers, eliminate rescuers and destroy vehicles and rescue equipment, or prevent a rescue operation involving parallel assassination.

Public administration facilities in which the state authorities responsible for counteracting, combating, identifying, or managing crises work are one of the main targets of terrorist attacks. Databases in these objects may also be at risk.

Systems of production, storage, and use of chemicals and radioactive substances are cost-effective objects of terrorist attacks. Effects of attacks using explosive charges or artillery means of the fire can cause extensive fires or freeing to the atmosphere of considerable toxic industrial funds poisoning amounts of substances causing mass poisonings of people or the contamination of the environment. Infiltration of smaller terrorist groups or single terrorists is quite simple due to the inaccurate protection system of an industrial plants.

As can be seen from above distribution, terrorists can hit land targets (stationary and mobile), water (on-shore, underwater, coastal and ocean) and aircraft. Land targets for terrorists may be various facilities located and operating on the terrestrial territory of a given state, including the military. The basic forms of terrorist attacks that may be carried out on critical infrastructure of the state include:

- bomb attacks; which means the use of explosives in the following manner: installation of an explosive device in or near a property, suicide attacks, attacks transport using the means of communication such as an airplane, a car, etc. Explosion loads can also be delivered to a critical infrastructure facility in the form of mail or supplies delivery. Explosives are the most common means used by terrorists to attack. It is conducive to the variety of explosives, their availability in some parts of the world, the ease of use and the spectacular effect of their use. In addition to explosives and industrial-scale equipment, terrorists also use improvised explosive device. The choice of the device depends primarily on the capabilities of individual terrorists and the terrorist groups and organizations from which they derive. The methods, equipment and materials used for the production of bombs and explosive devices are also dependent on the cultural traditions and conditions. The place of action or the origin of the perpetrators;
- short-lived fire influence with using small arms e.g. machine, of mortars and portable anti-aircraft rocket sets and armour-piercing rounds;
- abduction of staff (taking hostages) in order to obtain wealth (ransom) or obtain information about a given property. By kidnapping workers they can also force others, such as family members, diversionary and sabotage activities on critical infrastructure facilities;
- execution of attacks using NRBC (nuclear / radiation, biological and chemical) resources directly on or near the facility, eg the destruction of ammonia tank at the railway station;
- cyber-attacks on information systems in the form of: hacking into computers and general computer systems, i.e. hacking into information systems to achieve benefits; so-called Cracking- the use of a program that allows to enter the server within the omission of safeguards – it is backdoors - but also eavesdropping between the computers and sniffing passwords, impersonating other computers (IP

spoofing), phishing, logic bombs or most common worms and computer viruses.

IV. Protection of Critical Infrastructure of the State From Terrorist Threats

To ensure security of the facility, an appropriate system of should be constructed. This requires conducting operations that aim is full analysis of the object and quantify precisely the nature of potential threats. Therefore, to ensure the proper effectiveness of protective activities, it is desirable to create a security system in the facility, consisting of a number of different elements. This system is created to ensure the safety of persons, property and non-disrupted functioning of the object. In this regard, the concept of the object security should be presented. It can therefore be depicted as a variety of activities and the forces and means used in the facility to ensure the safety of people and property according to a specific concept, corresponding to threats and the current legal status. It is possible and so to introduce him as diverse action and powers and centres used in the object in order to assure safety of people and possessions according to the determined concept, meeting threats and the current legal status. The elements of the facility's security system are: physical security - a set of measures that minimize the risk of interference with the functioning of the critical infrastructure by unauthorized users. It consists of the protection of persons, understood as actions intended to ensure the safety of life, health and personal integrity, and the protection of property, namely measures to prevent acts of terrorism against property, and to prevent the occurrence of damage resulting from these events.

In this context, organizations need to be understood as "identifying, agreeing and implementing issues that define the principles and behavior of an object and the behavior of people in specific situations that are routine and specific in terms of security". Within this activity, the concept of the protection system and the basic documentation of it are developed. Further organizational activities include such issues as the organization of functional zones in the facility and rules for access to them, - placement of people and property, rules and organization of movement of people, vehicles and property, mode and manner to control traffic of persons, vehicles and property, co-operation with persons or entities from outside (supplies, social and technical support, co-operation, etc.). Also there should be distinguished equipment for protection and the rules for their use, the manner in which physical protection is used on daily basis and in special situations, the principles of cooperation with the Police and emergency service in the facility, corrections of the security system in the object, etc. The physical protection is also provided through: the fence, barriers i.e. concrete obstacles from prefabricated elements, - gates from steel profiles on the main and spare slip road; technical centres, domestic services and the system of the monitored access. In general, the critical infrastructure protection system can be considered as interoperability between three systems:

- peripheral protection system (perimeter) and open area of the object;
- property protection and traffic control system for people within the build-up area;
- a video monitoring system of publicly available facilities of cities, stadiums, stations, terminals, shopping facilities, production halls etc.

Technical protection means a set of ventures and procedures created to minimize the risk of disruption of functioning of critical infrastructure related to the technical aspects of the construction and operation of critical infrastructure facilities, equipment, installations and services, including technical protection measures. This means that the critical infrastructure technical protection covers the compliance of buildings, equipment, installations and services with applicable standards (eg. construction) and other regulations (eg. fire) to ensure safe use of critical infrastructure and the technical security of the facilities by using fences, barriers, CCTV systems, access systems etc. measures. Therefore, while speaking about technical measures which constituting the units of security system it should be thinking about:

- building measures, such as: walls, ceilings, floors, roofs, entrances, exits, stairways, communication lines, architectural layout of buildings, building elements directly adjacent to the building, typical windows and doors, fences and fences of various types, e.t.c;
- mechanical means, understood as means of reinforcing or protecting specific building elements and premises, and autonomous means of storing and transporting property. This is a very broad group of resources, often integrated with electronic components. These include, but are not limited to: "reinforced windows (reinforced windows, shutters, grates, blinds, roller blinds, foils, etc.), reinforcement of entrances (special doors, locks, padlocks, bars, blinds, etc.) (Steel and armored cabinets, safes, etc.), portable security devices (hand cassettes, steel containers, folders, etc.), storage rooms;
- electronic means for which the simplified division is as follows: tampering devices, burglar alarms, access control measures, fire signaling means, industrial television.

Personal protection that is a set of ventures and procedures aimed at minimizing the risk associated with persons who, through authorized access to critical facilities, facilities, installations and services, can cause disruptions in their functioning. This protection should therefore be linked to employees and other people temporarily located within the critical infrastructure (service providers, suppliers, visitors). Personal protection is provided by individual equipment in the armament and special equipment (anti-skid vests, protective clothing, personal medical equipment, etc.) and the development of appropriate procedures and actions.

IT network protection is a set of ventures and procedures aimed at minimizing the risk of disrupting the operation of critical infrastructure related to the use of IT networks. It

also means protection against cybercrime and cyber terrorism and effective countermeasures against such incidents.

Legal protection is a set of ventures created to minimize the risks associated with the activities of other economic, state or private entities whose activities could lead to disruption of critical infrastructure facilities, equipment, installations and services. It implies the use of legal tools that prohibit, through the ability to control and possibly block or limit board decisions to, for example, a hostile takeover, merger or sale of certain elements of the infrastructure, which may result in disruption of its functioning

Any legislation must be taken into account in the organization and functioning of the security system - from the generally applicable legislation to the rules at the lowest organizational level of the facility.

Legal regulations may concern such problems as:

- building, fire, energy, sanitary requirements;
- for storage the weaponry, use and transport of dangerous means (toxic, radioactive, explosive, flammable, etc.);
- rules of conducting with dangerous devices (electric, gauze, with the weaponry and the ammunition, etc.);
- organization of functioning of the object under the executioner of safety (regulations, plans, instructions, procedures, scopes of responsibilities, etc.);
- competences, tasks and responsibilities of described functional persons and departments of the margin of safety;
- activities of security physical powers, technical support and elements supporting them and their supervisors.

These elements of critical infrastructure protection are mutually intertwined and only used together can produce satisfactory results. For critical infrastructure protection to be effective, it should be implemented at all levels and be a joint effort of both governmental and local government and operators and owners of critical infrastructure, which will increase the level of security and reliability of critical infrastructure.

V. CONCLUSION

Ensuring the efficiency of the functioning of the broadly understood infrastructure of the state, in its technical part (manufacturing plants, energy, telecommunications, transport and communication) as well as social (health care, rescue and civil protection, etc.) in the face of terrorist threats is of particular importance. Contemporary terrorism is unpredictable in terms of form, scale, place and time, and the consequences of an attack can disrupt the functioning of the country's security and defense system and bring enormous losses in human, economic and even social potential. In this situation, there is a justified need for a holistic approach to the security of these systems and objects, especially as progressive globalization, through widespread media access and the widespread computerization of all areas of human activity create the conditions for terrorist organizations to reach critical infrastructures and to attempt to its destruction or damage.

State critical infrastructure facilities are essential to the functioning of society and the economy of the state, decisive for its vitality and the ability to manage and operate effectively. Therefore, systemic solutions are needed to ensure that critical infrastructure facilities of the state have the necessary level of protection and vitality. Hence the development of a critical infrastructure security concept of the state meets this expectation.

REFERENCES

[1] Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r., Dz.U. z dnia 21 maja 2007 r., art. 19, p. 1 i 2.

[2] S. Dubisz (red.), Uniwersalny słownik języka polskiego, tom 4, Wydawnictwo Naukowe PWN, Warszawa 2003, p. 619.

[3] T. Kotarbiński, Hasło dobrej roboty, Wiedza Powszechna, Warszawa 1975, p. 136.

[4] B. Hoffman. Oblicza terroryzmu, Grupa Wydawnicza Bertelsmann Media, Warszawa 2001, p. 12.

[5] B. Bankowicz, M. Bankowicz, A. Dudek, Leksykon Historii XX wieku, Kraków 1996, p. 87.

[6] P. Durys, F. Jasiński. Walka z terroryzmem międzynarodowym, Studio STO, Bielsko Biała 2001, p. 7.

[7] B. Szymczyk. „Głos Uczelni", Biuletyn Informacyjny Akademii Rolniczej we Wrocławiu, Vol.139 (2005).

[8] T. Aleksandrowicz, Terrryzm międzynarodowy, Warszawa 2008, p. 21.