Reducing the potential vulnerability of the society in case of a terrorist attack against critical infrastructure sites and facilities

Dimo Kirilov, Antoaneta Simeonova, Angel Krumov
Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences,
67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria[1]

***Abstract**: This article discusses the issues related to the planning of activities for ensuring the physical security of critical infrastructure sites. The critical infrastructure is considered as an important element of the national security of the country, and the criticality is determined by the interdependence between the individual elements and the dependence of the society on its normal functioning.*

***Keywords**: risk, national security, protection, critical infrastructure, terrorism.*

1. Introduction

The problem of critical infrastructure protection gained great international popularity in 2001 after the September 11 terrorist attacks in the United States. This made almost all countries that are at potential risk of terrorist threats to initiate and implement serious changes in their legislation both in the field of protection of critical infrastructure and in the direction of terrorism. Special programs for the protection of critical infrastructure are being created, which are growing into strategic plans and even national strategies. Special attention is paid to cross-border cooperation in order to reduce the risk of terrorist attacks on critical infrastructure.

The process of critical infrastructure protection is defined by the Bulgarian legislation (Disaster and emergency situations Protection Act), as: "A set of activities aimed at ensuring the normal functioning, continuity and integrity of critical infrastructures in order to prevent, reduce, mitigate or neutralize threats, their risks or vulnerability "[1].

The tasks and responsibilities of the competent institutions for counteracting terrorism and controlling the consequences of terrorist acts derive from the Counter-Terrorism Act, updated in State Newspaper. no. 103 of 27 December 2016, the National Counter-Terrorism Plan, accepted by Decision № 669 of the Council of Ministers of 02.11.2017 and the regulations governing their activities and their interaction with other state and non-state entities [2, 3] .

When it comes to the possible threat of a terrorist act against potentially dangerous critical infrastructure, it must be taken into account that terrorist actions are premeditated and planned in detail and bear the scars of an operation that reflects the specific objectives and motives of the executors and meets their capabilities.

In order to ensure permanent and adequate protection against the terrorist threat, it is necessary to build sustainable communication channels between state institutions, local authorities, non-governmental organizations, religious and ethnic organizations. Ministries, departments and local authorities perform their tasks in accordance with their action plans and the orders and directives of the respective managers.

2. Vulnerability of society in case of a terrorist attack

In today's security environment, the threat of terrorist acts is growing and the lives and health of the personnel living in the infrastructure of a critical site or facility, as well as of all citizens located in conventional civilian sites, are directly endangered.

As each object of the infrastructure performs different tasks and functions, a huge expert resource is needed for the collection and analysis of data on the real technical condition of all objects as a whole. This requires decision-making on a case-by-case basis and prioritization of sites. The next and most important step is to take adequate action to implement physical security measures against terrorism for critical infrastructure sites and facilities.

Analyzes of terrorist attacks in recent years have led to the derivation of some basic scenarios for terrorist activity. Here we will focus on terrorist acts by placing explosives that pose a serious threat and pose a risk to potentially dangerous critical infrastructure facilities, such as hydrotechnical facilities (HTF) and, more specifically, tailings ponds, which we will consider as a "priority object".

3. Analysis of the risk of a terrorist attack against hydrotechnical facilities (tailing ponds)

As we have already noticed, in recent years the protection of critical infrastructure has begun to become part of the national security policy of any modern and rapidly evolving society. At the same time, some accidents and incidents that occur at its sites give the impression that the measures taken to protect it are not effective enough.

The analysis of the risk of a terrorist attack against hydrotechnical facilities (tailings) requires the collection of a complete set of data on the investment project, the functions of the facilities, location, orientation, surrounding areas and areas adjacent to the regulated property.

The information generated as a result of this survey serves the experts and those responsible for the planning and design of such facilities to draw up a general plan of infrastructure and functions, assessment and prioritization of the most valuable assets and vulnerable areas.

Risk analysis is a necessary tool to help determine the level of protection as well as the design of protection measures. As it is practically impossible to design safeguards to achieve zero risk, the concept of "accepted risk" is accepted or more precisely defined and how this risk supports the risk analysis when deciding on the integration of physical security measures against terrorist attack in the facilities and adjacent infrastructure.

The developed methods aim to provide minimum measures for protection of the facilities by:

- increase of safe distances;
- design of constructions so as to avoid the phenomenon of progressive collapse;
- design of non-structural parts to reduce the risk of flying debris in case of an explosion or impact;
- development of computer-simulated incidents to support the security of the facilities;
- continuous video surveillance and notification.

The contribution of the Republic of Bulgaria in this area is expressed through the Order of the Ministry of Regional Development and Public Works № RD-02-20-6 of 19 December 2016 on the technical requirements for physical security of construction, which generally recommends methods of physical security against intrusion, published in State Newspaper, issue 1 of 2017 [4].

4. Ensuring a certain level of protection and reducing the potential vulnerability of society in case of a terrorist attack

In today's security environment, there are asymmetric threats and increased terrorist activity on civilian and critical infrastructure sites outside the conflict areas and often in NATO and European Union member states, which requires a new approach to security management for buildings and facilities.

For this purpose, it is necessary to develop documents and practical methodologies giving guidelines for defining an emergency project situation (specifically for each prioritized site), by predicting scenarios, preventing the causes, limiting the damage and dealing with the consequences of the incident in order to be achieved low levels of risk of loss of assets or human health and life.

The process of critical infrastructure protection consists of the following stages:

- Strategic planning – strategic planning for the protection of critical infrastructure is related to the development and implementation of strategies that reflect the state policy of the country in the study area and contain guidelines for future action. Each strategy, whether in the field of security, an element of which is the critical infrastructure or other problem area, indicates the ways to achieve the set strategic goals. Many of the strategies are implemented in addition to an action plan, which contains a set of key tasks that must be completed in advance by the relevant contractors through the necessary resources;

- Criticality identification – starts with defining a list of critical sectors. The criticality of a sector is determined by its place and importance in the supply chain of vital products and services, and by the potential, adverse, destructive impact that its disruption would have on it. As a general rule, when defining vital sectors in all countries, "the potential loss of human life, the economic, political and social consequences" are taken into account. The process of identifying critical infrastructure is directly linked to vulnerability assessment, interdependence assessment and threat assessment activities [5];

- Threat assessment – from the point of view of their nature, the threats for the objects of the critical infrastructure can be divided into the following main groups: natural disasters – earthquakes, floods, droughts, landslides, strong winds, dust storms, hail, etc .; fires – from intentional and unintentional actions of the human factor; accidents – in sites operating with nuclear, radiation, explosive and flammable materials, industrial toxic substances and toxic gases, and are the result of intentional and unintentional actions by human factors; epidemics and pandemics – by humans, animals and plants; catastrophes – space, aviation, railway, road, with vessels, as a result of intentional and unintentional actions, as well as the result of targeted human actions – terrorism. The detailed analysis of the threats for the objects of the critical infrastructure allows their timely neutralization and increase of the resilience of the system [6];

- Vulnerability assessment – is the degree of susceptibility of an object from the critical infrastructure to certain threats. Indicates a place (object, connection) in the system, which is characterized by a greater degree of susceptibility to the impact of threats. Vulnerability, in itself, does not generate adverse consequences, it is realized only when it is exposed to a threat;

- Assessment of interdependencies – in the context of critical infrastructure protection, interdependence is "a two-way relationship between the elements of critical infrastructure, and the degree of dependence is not necessarily the same in both directions." [7]. "There are four main types of interdependencies: physical, informational, geographical and logical (two infrastructure sites are logically interdependent if the state of one depends on the state of the other through some mechanism that is neither a physical nor an information or geographical connection). Different political, legal or regulatory mechanisms can lead to a logical relationship between the elements of critical infrastructure "[8];

- Risk assessment – the process of analysis and risk assessment is reduced to determining the nature and extent of risk as a function of danger, vulnerability and probability. "The risk of a certain object from the composition of the critical infrastructure is defined as a function of three parameters: threat to the object – it is expressed in its intensity and the probability of disaster, its intensity and nature; consequences – in the site of the direct impact of the disaster (direct losses); loss assessment – as a result of the mutual influence between the objects of the critical infrastructure (indirect losses).

  Direct losses are assessed on the basis of the following negative consequences: human losses – human victims; people with permanent disability; people affected by the disaster; material losses – includes all types of possible material losses, calculated in material terms; environmental consequences – pollution of terrains that require the intervention of specialized teams or hinder the operation of the terrain for a longer period of time. Indirect losses are the result of reduced production and supply of goods and services, due to disruption in the functioning and mutual influence of objects and systems (sectors) that ensure people's daily lives [9];

- Strategic decision-making – strategic decisions set the direction for the future development of critical infrastructure protection, have a lasting impact, require reforms, require rational restructuring, commit significant resources and create competitive advantages. The goals and strategies for protection of the infrastructure affect the advantages and disadvantages, the opportunities and threats, the spheres of action, etc. They are taken in the formation, selection, implementation, control and evaluation of a selected strategy.

5. Conclusion

The modern interpretation of the term "critical infrastructure" defines it as a system of facilities, services, information systems, the shutdown and malfunction or destruction of which would have a serious negative impact on the health and safety of the population, environment, national economy or the effective functioning of the State Management.

Due to previous perceptions of the safety of the operation of buildings and facilities, according to which they need to be protected only from natural forces and human error, there was a lack of legislation concerning safety in case of intentional human-caused accidents. Terrorist activity on the territory of NATO and European Union countries in recent years has sparked a wave of proposals to improve the security environment by improving urban, defense and critical infrastructure.

The analysis of the risk of a potential terrorist attack against hydrotechnical facilities (tailings) and the information generated as a result of collecting a complete set of data on the investment project, the functions of the facilities, location, orientation, surrounding areas and areas adjacent to the regulated property is a necessary tool to help determine the level of protection as well as the design of protection measures.

The results of this report are aimed at the implementation of Work Package 2 “Intelligent Security Systems” of the project BG05M2OP001-1.002-0006 “Construction and development of a Center of Competence “Quantum communication, intelligent security systems and risk management (Quasar)““, which has received funding from the European Regional Development Fund through the Operational Program “Science and Education for Smart Growth” 2014-2020.

Literature:

1. Disaster and emergency situations Protection Act, updated State Newspaper no. 102 of 19 December 2006, as changed State Newspaper no. 41 of 22 May 2007, as changed State Newspaper no. 113 of 28 December 2007, as changed State Newspaper no. 69 of 5 August 2008, as changed State Newspaper no. 102 of 28 November 2008, as changed State Newspaper no. 35 of 12 May 2009, as changed State Newspaper no. 74 of 15 September 2009, as changed State Newspaper no. 93 of 24 November 2009, as changed State Newspaper no. 61 of 6 August 2010, as changed State Newspaper no. 88 of November 9, 2010, as changed State Newspaper no. 98 of 14 December 2010, as changed State Newspaper no. 8 of January 25, 2011, as changed State Newspaper no. 39 of 20 May 2011, as changed State Newspaper no. 80 of 14 October 2011
2. Counter-Terrorism Act, prom. DV. no. 103 of 27 December 2016, available at https://www.strategy.bg/
3. National Counter-Terrorism Plan, accepted by Decision № 669 of the Council of Ministers of 02.11.2017, available at https://www.strategy.bg/
4. Order of the Ministry of Regional Development and Public Works № RD-02-20-6 of 19 December 2016 on the technical requirements for physical security of construction works, published in State Newspaper no. 1 of 2017
5. Drakalieva, P., Ivanov, I., Problem analysis of critical infrastructure, project “Protection of critical infrastructure in the EU and Bulgaria – economic and organizational aspects”, Department of National and Regional Security, UNWE, Sofia, 2008, pp. 19-20
6. Methodology for modeling, analysis of critical infrastructure, identification of interdependencies, assessment of vulnerabilities and risk and planning of protection capabilities, Research report, BAS, Sofia, 2005, article
7. Homeland Security – National Infrastructure Protection Plan, USA, p.118
8. Kirov G., Stoyanov V., Simulation approach for analysis and assessment of the interdependencies between the elements of the critical infrastructure, in “Second National Scientific and Practical Conference on Emergency Management and Protection of the Population”, BAS, Sofia, 2007, article
9. Hadjitodorov S. and team, Methodology for assessment of critical infrastructure at the municipality level, in the Second National Scientific and Practical Conference on Emergency Management and Protection of the Population, BAS, Sofia, 2007, article