PROTECTION OF CRITICAL INFRASTRUCTURE FROM TERRORISM

Gjorgji Veljovski
Military Academy ‘General Mihailo Apostolski’- Skopje, Republic of Macedonia
gveljovski@yahoo.com
Metodija Dojchinovski
Military Academy ‘General Mihailo Apostolski’- Skopje, Republic of Macedonia
m_dojcinovski@yahoo.com

Abstract: The attacks on critical infrastructure could seriously jeopardize national and international security and disturb the overall normal way of life of the population. It could cause massive losses, weaken the economy, break public morale and people’s confidence in the government. The characteristic of the modern terrorism is a strategy to inflict as much damage as possible to the state and the population. Disabling or destruction of infrastructure that is identified as critical for the life of the state is a high-value target. Besides the existing security risks to critical infrastructure such as natural disasters and human errors, the danger of terrorist attacks pushed the states further to take specific measures to defend it. Its protection against terrorist attacks has become not only important but also necessary because states today are energy-related and safe operation of their critical infrastructure directly affects the national and international security. States need to build consistent, national approach to protect critical infrastructure from terrorism by taking specific measures at national level, with particular attention to ensure regional energy security as a factor for the regional stability. The purpose of this article is to overview the aspects of challenges, vulnerabilities, and ways to organize the protection of critical infrastructure from terrorist attacks. When it comes to protection of critical infrastructure from terrorism, it is inevitable to centralize security and the private sector. Given the possible consequences for the population, economy, politics and other aspects of society on which national security depends, the state must delegate obligations to the private sector that owns facilities, systems, and installations that have been identified as a critical. In return, the state should support the private sectors with access to all necessary information on terrorist threat assessment because it is the key tool for prevention and setting of adequate protection.

Keywords: critical infrastructure, terrorism, vulnerability, security, protection.

1. INTRODUCTION

In the last three decades, modern terrorism has turned into a global, transnational threat. As the extreme form of violence freed of all moral values, terrorism is among the priority security threats to most of the states in the word. Disabling or destroying the infrastructure identified as critical for the life of the state is highly costly, therefore potentially the most desirable target of any terrorist. As states became energy dependent and increasingly interconnected, the safe functioning of their critical infrastructure directly affects national and international security. Its protection from terrorist attacks has become not only important but also necessary. There is a growing concern in looking at the vulnerability aspects of the critical infrastructure and how to organize its protection against the possibility of terrorist attacks.

In addition to other potential security challenges, the danger of terrorist attacks has greatly contributed that states exactly define what represents a critical infrastructure.[230] Protection of this type of threat varies by ways and means in relation to vulnerabilities of another type, such as natural disasters, human errors or system failures with greater consequences. Because of unavoidable risk that these types of threats can damage critical infrastructure, they are considered the acceptable statistical probability (for example, a Tsunami hitting the nuclear plant in Fukushima).

However, terrorism is a planned, deliberate act of armed violence aimed at deliberately damaging or destroying targets that can cause catastrophic consequences. Modern terrorism seeks spectators and as many victims as possible, making critical infrastructure an extremely tempting target for terrorist groups and organizations. Significant parts of the critical infrastructure are all those facilities and systems that enable the state's energy security. States have to build long-term security strategy, implement protective measures and continuously invest in increasing their safety against terrorist attacks because it could have a negative impact not only on the national security but also for the international.

2. DEFINING THE PROTECTION OF CRITICAL INFRASTRUCTURE AS A SECURITY ISSUE

It is essential to identify what exactly is the critical infrastructure of the state, in order to choose the right strategy and to apply effective and most economical methods to protect it from terrorism. Furthermore, it is

[230] Robert Radvanovsky and Allan McDougall. (2010).*Critical Infrastructure: Homeland Security and Emergency Preparedness*, Second Edition, CRC Press, FL., 6.

necessary to make a risk assessment, either the extent of certain damage caused by a terrorist attack or the awareness what could be lost in case of total destruction. In the end, to design effective protection, states should develop several possible and realistic scenarios of terrorist attacks on their critical infrastructure. Critical infrastructure refers to complex systems in the state that provide products and services that are necessary for everyday life. Not all systems are critical, and there is often too much ambiguity in their identification. In some cases, systems that are not absolutely critical are designated as such. This can cause additional financial costs for their protection and distract the security from the truly critical systems.

There are many definitions of critical infrastructure. Most of them include elements such as: energy sources and facilities, communication systems, various public services such as finance, food distribution, healthcare, transportation, various aspects of public safety such as nuclear protection, search and rescue and emergency assistance, the government of the state and its capacities, administrative buildings, various commercial buildings, nuclear power plants and dams. Critical infrastructure is everything that must function to provide the basic public services on which the life of the state depends. Particularly the telecommunications and flow of information is an indispensable segment to ensure the functioning of the economy, production and development, and important to connect other sectors in the society. Public transportation is especially important for the everyday life and work of citizens and the functioning of all social activities. It is therefore, the most common target of terrorist attacks in the last few decades, from the 1995 sarin gas attacks in Tokyo[231] to the latest attacks in Madrid 2004, London 2006, Paris 2015 and Brussels 2016.

It is obvious that these are so complex systems that the effects of a possible terrorist attack would have wider, long-term consequences difficult and expensive to return to the original state. The US has the wider definition of critical infrastructure, with the longest period of recognition as a security matter. The notion of critical infrastructure extends at many other sectors such as agriculture and food industry, water production, health, energy, transportation, banking, chemicals, postal services and shipping, sectors that are necessary for the economy, and emergency services necessary to function in peace or crisis.[232]

The first attempt of the US government to define critical infrastructure was in 1983 after the US faced the first massive casualty terrorist attack on the Marine building in Beirut, Lebanon.[233] In the annual report of the Congressional Budget Office, it was pointed out that all those facilities in which it is invested from the federal budget should be considered critical to the national security as their damage, disability or destruction is intended to cause direct damage to the economy".[234] In the coming years, the definition of critical infrastructure in the US has expanded and encompassed all physical elements used to provide a public service that should last for years, such as roads and bridges, airports and runways, public transportation systems, wastewater and water supply systems, hospitals, government buildings, communication facilities, railways and all other federally funded facilities and institutions.[235] Furthermore, this definition was expanded to include all high-cost objects planned to last as a long-term economic investment, is related to economic development or has to do with the development of the public sector, all services that can provide forms of protection within the national defense, strengthening the economy, protecting the health and safety of people.[236] Such national infrastructure is so important that its disabling or destruction would have major consequences on the economic stability.

With the development of computer technology and the Internet, cyber systems are part of the critical infrastructure as it became clear that they are also essential for the functioning of the economy and the government. This covers all systems and subsystems, physical or cyber that are so important to the nation that their disabling or destroying has a negative impact on national security, the development of the national economy and national health insurance and security. The definition of critical infrastructure was then extended to telecommunications, energy systems, financing, food production, water, transport, health insurance and emergency services. Within their frameworks, cyber and communication systems are considered critical because they must remain operational at any time to ensure continuity of work. Their disability would be critical to national and economic security, public health and the physical stability of the population.

[231] Benjamin Cole. (2011). The changing face of terrorism: How real is the threat from biological, chemical and nuclear weapons? Tauris. London, 17.

[232] Brian T. Bennett, (2007). *Understanding, assessing, and responding to terrorism*. John Wiley & Sons, Inc., Hoboken, New Jersey, 53.

[233] Bret Stephens. (2012). Iran's Unrequited War. The Wall Street Journal. October 22 http://www.wsj.com/articles/SB10001424052970203630604578072452443447568

[234] Bennett, 51.

[235] Bennett, 52.

[236] Bennett, 52.

3. TERRORISM AS A SPECIFIC THREAT TO CRITICAL INFRASTRUCTURE

Although there are many definitions of terrorism, its nature is clear and most of them gravitate around the evident concept of planned armed violence for the purpose of achieving political goals. Terrorists are usually non-state actors that are aiming at the security of the civilian population in order to pressure the government of the state to respond to their demands. By definition, the terrorists seek high-value targets. While in the 80s the main characteristic of a terrorist attack was to kill a few to frighten many, today this has changed significantly, mainly because of the expansion of religious extremism. It is increasingly evident that a rising trend is terrorist attacks that seek to cause as much damage as possible.

Today's terrorists seek various and creative ways of killing as many people as possible. The ideal way of doing this would be the use of weapons of mass destruction. There is plenty of evidence that over the past three decades several terrorist groups and organizations have tried to obtain or produce some kind of weapons of mass destruction.[237] Once the terrorists have realized that it takes a long time and is almost impossible, there is an evidence of several attempts to make improvised weapons of mass destruction.[238] Once it became apparent that this was also practically unfeasible, the only possibility to cause mass casualties was to produce indirect effects by attacking a critical infrastructure. Its damage or destruction, depending on the type, could cause damage with catastrophic consequences.

Although terrorists in the past relied on light weapons and guerrilla tactics of improvisation, they increasingly take advantage of the sophisticated armament, new technologies, and computers. Today's terrorists are more educated, more informed, more capable and do not resemble terrorists from the 70s and 80s that had limited goals. Statistics show that more and more of their members include highly educated personnel with knowledge and skills from different fields of science. The targets of the terrorists are various but often chosen to be feasible. Based on their probability to succeed, they can be light and heavy or targets easy to attack and targets that require more time for planning, forces, and resources. Attacks on the state's critical infrastructure would be desirable because in that way the terrorists could simultaneously achieve more effects.

Disabling an infrastructure that is important for the functioning of the state has a great psychological impact on the population because it can inflict multiple human casualties. If a direct blow to the state's economy is achieved, it could seriously undermine the authority of the government due to the inability to protect the critical infrastructure and the population. Terrorists will try to attack the critical infrastructure to achieve all these goals. A particularly dangerous attack would be on the food industries, transport and energy sources. However, the terrorists know that the critical infrastructure represents a "hard target"[239] that is well secured and protected. Nuclear power plants, energy sources, airports and government buildings are under special protection and their security measures are increasing with every subsequent attempt for a terrorist attack.

Precisely because they are well protected, terrorists are becoming more persistent in trying to break the protection. Believing that the government should protect such facilities, a successful terrorist attack on critical infrastructure would make the citizens much more uncertain. The effects of such an attack are multiplied because they would compromise the ability of the state to protect essential objects. It is already clear that terrorist groups and organizations view terrorism not only as armed violence but as a long-term strategy for achieving their goals. For this reason, they recognized the psychological effect of terrorism. The very idea that an attack on a chemical or a nuclear power plant is possible, causes not only fear among the population but also material damage. The threats of terrorism make governments commit large assets to protect and secure facilities that, if targeted, may have catastrophic secondary effects on the civilian population and the natural environment.

The US is the appropriate example of taking measures to protect critical infrastructure from terrorist attacks. Apart from having the most developed infrastructure, it is a desirable target for many terrorist organizations. The protection of critical infrastructure has become a special topic of discussion after the attacks of September 11. It became apparent that the new concept of modern terrorism aims at inflicting mass casualties and economic damage. Terrorists chose to attack the World Trade Center as a symbol of the economic power of the United States. For the European countries, the urgency for a deeper analysis and implementation of policies to protect critical infrastructure has intensified after the attacks in Madrid 2004 and London 2006.[240] The safe operation of the railway system in the major cities of Europe is essential and necessary for the normal life of the population.

In trying to develop the most effective protection strategy, three types of catastrophic attacks on critical infrastructure have been identified: attacks that can occur "from the inside", "from the outside" or in

[237] Benjamin Cole, 60.

[238] Thomas Graham Jr. Keith A. Hansen. (2009) Preventing Catastrophe. The Use and Misuse of Intelligence in Efforts to Halt the Proliferation of Weapons of Mass Destruction. Stanford security studies. Stanford University Press, California, 18.

[239] Bennett, 62.

[240] 162 CDS 07 E REV 1 - The protection of critical infrastructures, Lord Jopling, UK, special reporter

collaboration with outside actors with help from the inside.[241] The critical infrastructure can be static or mobile, and the attack on it could be a physical or cyber-attack since today all systems are software-linked in a network. The terrorist use of cyberspace is one of the new characteristics of modern terrorists. While the physical attack is immediate and direct, the cyber-attack can be done indirectly at a greater distance. From the aspect of the attacker, both have good and bad sides; therefore from the aspect of the defender both require different operational approach. What must be considered is the fact that the modern terrorist groups and organizations are highly adaptable, flexible and creative in finding new ways to cause greater damage.

4. VULNERABILITY AND THREAT ASSESSMENT FROM A TERRORIST ATTACK ON A CRITICAL INFRASTRUCTURE

The attacks on critical infrastructure could seriously jeopardize national and international security and disturb the overall normal way of life of the population. It could cause massive losses, weaken the economy, break public morale and people's confidence in the government. The criticality of the infrastructure is measurable primarily in terms of how much the population and the state dependent on it, or the bigger dependence, the more important it is. The second factor is the vulnerability or the more vulnerable it is, it is more critical because it can be easily lost. Third, the lack of alternatives is considered as critical, because when disabled or damaged, it would be difficult to replace it.

Providing security for the critical infrastructure is important for every state. The challenge is that due to the transnational connection of the power grid and pipelines, they are usually dependent on one another. Because of this, each state has an obligation to the neighbors around it to protect its own critical infrastructure from terrorist attacks. The problem is complicated if sometimes, a good portion of the critical infrastructure is in the hands of the private sector (for example, in the US, as much as 85%).[242] However, even if it is not a state investment, it remains essential for the functioning of the state. This raises many questions about the manner in which it is secured and the role of the state in relation to private management or the achievement compatibility of national security with business interests.[243] The private sector is often more interested in maximizing the profits, sometimes at the expense of maximum protection.[244]

The fact that the critical infrastructure is usually widespread throughout the state additionally complicates its protection. It gives the potential attackers freedom of maneuver, and for the defender, it imposes a more expensive and more complex approach to organize the protection. Therefore, in order to secure and successfully defend the critical infrastructure, prioritization of potential targets is needed. The premise of the protection comes from the necessity to function in all conditions besides all existing vulnerabilities. The threat of terrorist attacks additionally complicates the process because the more vulnerability the system has, the bigger probability that something will be omitted and more options are available for the terrorists. Computer technology facilitates the operations of these systems, but at the same time, it makes them vulnerable. There are no longer independent systems and all of them are in some way interconnected and interdependent.[245] Vulnerabilities may occur in many forms, from human error, hardware, software, weather conditions, etc. States that are technologically advanced are actually more vulnerable to terrorist attacks, especially from cyber-attacks.[246]

The essential part of the process of protecting critical infrastructure from terrorist attacks is the evaluation, analysis, and elimination of potential vulnerabilities. Although absolutely nothing can be foreseen, it is preferable to reduce the possible options. The challenge is that sometimes, due to the price they impose to prevent them, seemingly unrealistic scenarios are overlooked and the necessary measures are not taken. The terrorists may search for a particular vulnerability in the system, that was assessed the least probable and therefore unintentionally left as a security gap. For example, the danger of a passenger airplane crashing on a nuclear power plant is one of these scenarios. Although they have concrete protection, it should not be excluded that some terrorists may obtain sophisticated weapons that could penetrate the defense. Terrorist groups like Hezbollah and Hamas have already demonstrated to have missile capabilities, which mean it is likely that in the future some terrorist groups could attempt to attack a nuclear power plant.

In securing any object that is a potential target of a terrorist attack, various early detection methods are used to prevent the attack. One method for planning the protection of the critical infrastructure is to draw up an

[241] Bennett.
[242] Bennett, 57.
[243] 162 CDS 07 E REV 1 - The protection of critical infrastructures, Lord Jopling, UK, special reporter
[244] Laurie Anne Schintler, Sean Gorman, Rajendra Kulkarni and Roger Stough, *Moving from Protection to Resiliency: A Path to Securing Critical Infrastructure* in Alan T. Murray · Tony H. Grubesic (Editors) Critical Infrastructure Reliability and Vulnerability, 291.
[245] Robert Radvanovsky and Allan McDougall, 3.
[246] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?", Routledge, 2005, 130.

assessment matrix.[247] There are many indicators that terrorists want to commit an attack that is revealed by observing certain unusual behaviors around the facility. For example, if third parties show a particular interest in the object, there are traces of information requests for vulnerability assessment, or attempts to break into security systems - which would mean testing security or actual intrusion or entry into objects. Other indicators that the object is of interest to attack are traces of collecting means of attack such as the purchase of large quantities of fertilizer or other substances with which an improvised explosive device can be made, the presence of suspicious persons near the facility and even trial attempts attack.

To make realistic security assessments while planning the protection of the critical infrastructure, a realistic perception is necessary on the potential threat of specific terrorist groups and organizations. For accurate risk assessment and building an effective security system, it is crucial to understand the characteristics of the potential terrorist group, its capabilities, limitations, tactics and previous experience.[248] Detecting or at least suggesting potential attackers can make an analysis of the level of threat based on terrorists' motives. One of the methods for assessment, evaluation, and analysis of the critical infrastructures' vulnerabilities from terrorist attacks is a penetration test. Terrorism experts in the US apply this by physical and technical penetration through the protection of facilities and systems.[249] Based on counter-terrorism experiences, they perform object analysis, identify their weaknesses, and advise the operators how to improve the security protocols. It is considered that if such tests are done more often, it will keep operators of critical infrastructure alert and more aware of the possibility of being surprised by a terrorist attack.

5. EXAMPLE OF VIABLE NATIONAL STRATEGY

The Western countries have a similar set of measures to protect their critical infrastructure from various threats. Regarding the possibility of attacks from terrorist groups and organizations, states cooperate and share the experience. Most of the counter-terrorist measures overlap: developing a national plan, designating central body responsible for protection, increased level of awareness, threat assessment and identification of vulnerabilities, cooperation between institutions for information exchange, preventing cybercrime and international cooperation to protect the transnational infrastructure.

States need to build consistent, national approach to protect critical infrastructure from terrorism by taking specific measures at national level. Some governments already identified that it is important to demand responsibility for protecting critical infrastructure from owners and operators.[250] The private sector that controls the infrastructure designated as critical, needs to understand terrorism as a specific threat and to include it when developing a risk assessment. At the same time when the state government delegate responsibility, it should provide necessary legal regulations, intelligence and institutional assistance to help private sector facilitate protection.

An example of cooperation between the state and the private sector that owns parts of the critical infrastructure in taking counter-terrorist measures are the national guidance from the Australian government,[251] binding the owners to follow the protective measures defined for certain degree of alertness. Owners are obliged to maintain the level of awareness against terrorism, regularly carry out risk assessments and safety control, train employees, conduct security exercises and report on incidents and suspicious activities around the infrastructure. They also must apply risk management techniques in the planning process and have emergency plans for different situations including terrorism.

When it comes to protection of critical infrastructure from terrorism, it is inevitable to centralize security and the private sector. Given the possible consequences for the population, economy, politics and other aspects of society on which national security depends, the state must delegate obligations to the private sector that owns facilities, systems and installations that have been identified as a critical infrastructure. In return, the state should support the private sectors with access to all necessary information on terrorist threat assessment because it is the key tool for prevention and setting of adequate protection.

6. CONCLUSION

In essence, the precarious trend of international terrorism has prompted states in the 90s to think about what exactly is a critical infrastructure. Until then, everything that was built for the functioning of society was considered to be important. However, with the threat of terrorism and apocalyptic scenarios in which terrorists

[247] Bennett, 70.
[248] John Sullivant, *Strategies for Protecting National Critical Infrastructure Assets A Focus on Problem-Solving*, 155.
[249] Robert Radvanovsky and Allan McDougall.
[250] *National guidelines for protecting critical infrastructure from terrorism*, Australia-New Zealand counter-terrorism committee, Commonwealth of Australia 2015.
[251] *National guidelines*, 13.

could cause enormous damage and casualties if they attack certain targets, some infrastructure has been identified as critical for national security.

In addition to regular protection from natural disasters and human mistakes, states invest in the security of the critical infrastructure because of the emerging threat from terrorism. Counter-terrorism became an essential part of the national security strategy, with special attention to ensuring regional energy security as a factor for regional stability.

The security of the critical infrastructure, especially the energy sector, directly affects wider security because these systems are interconnected. Certain targets if attacked can cause far more catastrophic consequences for the people and the state, therefore have been identified as critical even when they are owned by the private sector. Because disruption of the critical infrastructure in one state could undermine wider regional stability, its protection in the future will require not just national, but also regional efforts. Designing a viable national strategy that includes delegating responsibilities to the private owners will be crucial to have efficient protection from possible terrorist attacks.

REFERENCES

[1] Benjamin Cole. (2011). The changing face of terrorism: How real is the threat from biological, chemical and nuclear weapons? Tauris. London.

[2] Bret Stephens. (2012). Iran's Unrequited War. The Wall Street Journal. October 22 http://www.wsj.com/articles/SB10001424052970203630604578072452443447568

[3] Brian T. Bennett, (2007). *Understanding, assessing, and responding to terrorism*. John Wiley & Sons, Inc., Hoboken, New Jersey.

[4] Gabriel Weimann, “Cyberterrorism: The Sum of All Fears?”, Routledge, 2005.

[5] John Sullivant, *Strategies for Protecting National Critical Infrastructure Assets A Focus on Problem-Solving*.

[6] Laurie Anne Schintler, Sean Gorman, Rajendra Kulkarni and Roger Stough, *Moving from Protection to Resiliency: A Path to Securing Critical Infrastructure* in Alan T. Murray · Tony H. Grubesic (Editors) Critical Infrastructure Reliability and Vulnerability.

[7] *National guidelines for protecting critical infrastructure from terrorism*, Australia-New Zealand counter-terrorism committee, Commonwealth of Australia 2015.

[8] Robert Radvanovsky and Allan McDougall. (2010).*Critical Infrastructure: Homeland Security and Emergency Preparedness*, Second Edition, CRC Press, FL.

[9] Thomas Graham Jr. Keith A. Hansen. (2009) Preventing Catastrophe. The Use and Misuse of Intelligence in Efforts to Halt the Proliferation of Weapons of Mass Destruction. Stanford security studies. Stanford University Press, California.

[10] 162 CDS 07 E REV 1 - The protection of critical infrastructures, Lord Jopling, UK, special reporter