ROMANIAN
MILITARY
THINKING

TERRORISM AND ORGANIZED CRIME – 21ST CENTURY THREATS TO CRITICAL INFRASTRUCTURES. AN ANALYSIS OF MOTIVATIONS AND *MODUS OPERANDI*

Lieutenant Colonel Ionuț-Cosmin BUȚĂ, PhD
"Carol I" National Defence University, Bucharest
10.55535/RMT.2024.2.7

In today's world, where globalization has led to the emergence of various state and non-state actors, including sub-national ones, with differing interests and motivations that often conflict with one another, the provision of essential services such as transportation, electricity, drinking water, medical and digital services, and others is of critical importance to contemporary society. About half a decade ago, when the critical infrastructures that provide these services were built, threats to them, such as terrorism, organized crime, asymmetrical or hybrid ones, were almost non-existent and not as much of a concern to the critical entities responsible for protecting them.

The present research is intended to carry out an analysis of two threats to critical infrastructures – terrorism and organized crime, with the aim of identifying their typology, the effects they produce, the method of operation employed by the non-state actors that conduct such activities.

The article's findings have demonstrated that ideological, political, and religious motivations of terrorist organizations, as well as the financial motivations of organized crime hold special significance as they yield effects in the modus operandi of these entities and also shape the response of law enforcement authorities.

Keywords: organized crime; terrorism; critical infrastructures; essential services; critical entities;

INTRODUCTION

The increase in the level of interconnectivity and the dynamics of vulnerabilities and threats to critical infrastructures have determined that the scope of critical infrastructure security should acquire new valences (National Critical Infrastructure Security Liaison Officer's Handbook, 2021) in increasingly diversified fields. Within these new types of threats, terrorism and organized crime have taken on new dimensions that require different approaches and resource allocations compared to previous periods. Moreover, in many countries, since the 1980s and 1990s, the transfer of key elements of critical infrastructure to private companies has been achieved. (Boin, Smith, 2006, p. 295).

The increase in the level of interconnectivity and the dynamics of vulnerabilities and threats to critical infrastructures have determined that the scope of critical infrastructure security should acquire new valences in increasingly diversified fields.

Under these conditions, the privatization of these companies has produced another dilemma due to the critical nature of the infrastructures. Although these infrastructures are of major importance in the framework of public management, they have moved out of the close sphere of control of state actors with the transfer of ownership from the public to the private sector (Ib., p. 296). This shift has made critical infrastructures possible targets for both state and non-state actors, such as terrorist organizations and organized crime (Riedman, Warden, 2017, p. 19).

This fact has brought benefits in terms of administration and private management, but it has also created new vulnerabilities, especially in the sphere of preventing and combating terrorism. In many cases, the fear of a possible terrorist attack paralyzed the operation of critical infrastructures for certain periods, as demonstrated by the false alarms following the 9/11 attacks (Boin, Smith, ib., p. 297).

TERRORISM – A THREAT TO CRITICAL INFRASTRUCTURES

Within the framework of research related to the impact of terrorism on critical infrastructures, there are three main approaches:

- the terrorist threat that uses non-lethal methods and means, namely the cyber threat (Lewis, 2002; Haimes, Longstaff, 2002; Shea, 2003; Chittester, Haimes, 2004; Wilson, 2014; Bologna, 2015);
- the lethal terrorist threat, or brute force, explosive devices, light weapons, vehicles etc. (Stewart et al., 2006; Frolov, Baecher, 2006; Patterson, Apostolakis, 2007; Stewart, Mueller, 2020);
- the terrorist threat that uses both non-lethal and lethal methods (Bennett, 2018).

Mueller and Stewart compare the financial damages of the 11 September 2001 terrorist attacks on the World Trade Center with those of natural disasters over time for which there is reliable information.

Terrorist acts share similarities with natural hazards but are distinguished by the malicious use of all the synergies they can produce (Apostolakis, Lemon, 2005, p. 361).

In this context, Mueller and Stewart (2011) compare the financial damages of the 11 September 2001 terrorist attacks on the World Trade Center with those of natural disasters over time for which there is reliable information. They find that the destruction caused by the 9/11 attacks resulted in approximately $123 billion in financial damages, far exceeding those caused by any natural disaster.

In an ideal environment, critical infrastructures would only be affected by minor errors. However, because of the impact of globalization on society, the technological developments and the easy access to disruptive technologies, threats such as terrorism and organized crime are increasingly present in critical infrastructures. This necessitates constant efforts to stay ahead of new types of actors (Pîrjol, Chisega-Negrilă, 2020, p. 14).

Boin and Smith (2006, p. 297) argue that most public state organizations, and especially private ones, lack administrative structures and have not developed processes to mitigate the risks

of a crisis caused by a terrorist event. They identify the challenges these organizations face in implementing measures to prevent and combat terrorism, such as:

- the impossibility of preventing and taking preparation measures against possible attacks;
- the ability to implement an early warning system;
- the decision-making capacity in crisis situations;
- the ability to respond to the crisis through measures of coordination, communication, management of complex events and public-private networks;
- the ability to return to the situation existing before the crisis.

Stewart and Mueller (2020, p. 1) analyse terrorist risks to critical infrastructures by examining the number of victims from attacks involving the use of lethal ammunition, explosives, or vehicles, correlated with the probability of death risks.

Stewart and Mueller analyse terrorist risks to critical infrastructures by examining the number of victims from attacks involving the use of lethal ammunition, explosives, or vehicles, correlated with the probability of death risks.

Analysing recent terrorist events, Stewart and Mueller (ib., p. 10) argue that a large-scale terrorist attack like the one on 11 September 2001 is not a predictor of similar future events but contributes to spreading panic and fear among the population. They note that the attacks in Madrid and London in 2004 and 2005, which involved explosive materials, were not followed by similar events in subsequent years. Instead, terrorist groups have used light weapons and vehicles to achieve their objectives. It suggests that, for terrorist organizations, the primary goal is not the specific target of the attack, but the message and magnitude of the event created through that target. The target is merely a means to produce an effect, and if the same effect can be achieved through a cyber attack, then that will likely be the means used.

Other researchers have focused in their analyses on the interpretation of the terrorist phenomenon from the perspective of the organizational capacity they have developed to which Zoli et al, (2018) attribute the name *"terrorist critical infrastructure"* (TCI). In their interpretation, the concept of TCI represents those physical or virtual systems or assets designed and appropriated by terrorist

actors to achieve certain objectives (Zoli et al., ib., p. 1). Stewart et al. (2006) analyse the correlation between critical infrastructures and the terrorist threat starting from the premise that this threat materializes through the use of explosives. Thus, they analyse the impact of the terrorist phenomenon on critical infrastructures from the perspective of the effects produced by the explosions caused by this threat and perform a probabilistic risk assessment that can be used to reduce the effects of explosion damage on critical infrastructures.

In the same context, Frolov and Baecher (2006, p. IX) appreciate that terrorist attacks represent those events that are very well planned and carried out on targets that can cause a strong social response. Therefore, they consider it an urgent measure to develop techniques and methods to estimate which the most likely targets for terrorist organizations are.

Rudner emphasizes the effects of terrorist attacks on public opinion and believes that a possible successful terrorist attack on critical infrastructure can erode public trust in the authorities. In this regard, the author considers that even an attack of this kind carried out on critical infrastructure on the territory of Canada can produce this type of effect on the territory of the United States of America and vice versa.

Rudner (2009, p. 777) emphasizes the effects of terrorist attacks on public opinion and believes that a possible successful terrorist attack on critical infrastructure can erode public trust in the authorities. In this regard, the author considers that even an attack of this kind carried out on critical infrastructure on the territory of Canada can produce this type of effect on the territory of the United States of America and vice versa (Ib.).

Patterson and Apostolakis (2007) use Geographic Information Systems (GIS) to correlate the geographical location of critical infrastructures and classify the geographic regions where these infrastructures are located according to the probability of terrorist acts. This classification provides decision-makers with the necessary information to manage the resources allocated for preventing and combating terrorism on critical infrastructures in correlation with the identified vulnerabilities.

Yao et al. (2020, p. 1), following the analysis of a case study of a *power-supply substation*, suggest that when the threat is solely of a terrorist nature, improving critical infrastructure protection measures is more effective than enhancing the redundancy of that critical infrastructure. Cyberspace represents the nervous system of a country,

composed of hundreds of thousands of interconnected computers, servers, routers, and networks that contribute to the functioning of critical infrastructures (Bush, 2003). All these devices in cyberspace, which control physical objects such as public transport networks, electrical stations and transformers, warehouses, fuel pumps, and more (Ib.), along with the Internet of Things (IoT), contribute to the operation, protection, and resilience of critical infrastructures (Pătrașcu, Nicoară, 2023). These technologies create both vulnerabilities and benefits for states, as they contribute to the increase in the gross domestic product and improve the quality of life for their citizens (Chittester, Haimes, 2004, p. 1).

Haimes and Longstaff (2002, p. 443) argue that the physical and cyber vulnerabilities of critical infrastructures cannot be interpreted separately within civil sectors compared to those of national security. It is because the strong dependencies between them, particularly in the realms of security and civil infrastructure, which can lead to cascading effects that amplify risks to critical infrastructures.

Cyber terrorism is a method by which actors can create a strategic vulnerability. Therefore, much of the early literature on cyber attacks is similar in description to the literature analysing air attacks on critical infrastructure in the two world wars.

Cyber terrorism is a method by which actors can create a strategic vulnerability. Therefore, much of the early literature on cyber attacks is similar in description to the literature analysing air attacks on critical infrastructure in the two world wars (Lewis, 2002, p. 2). Starting from this idea, the author compares the air attacks of the First and Second World Wars, when strategic bombing of critical infrastructure such as power stations or factories of military equipment and armaments created the same effects as cyber attacks today (Ib.)

ORGANIZED CRIME – A THREAT TO CRITICAL INFRASTRUCTURES

Although it does not receive as extensive analysis in specialised literature as the terrorist threat, organized crime plays a significant role in the analysis of threats to critical infrastructures, given that these infrastructures are major sources of financial resources. Marjanović and Nađ argue that, regarding the threat of organized crime on critical infrastructures, there are insufficient measures in place to protect

them and mitigate the risks posed by such criminal activity (2013, p. 77).

Moreover, the Europol report (EU SOCTA 2021) identifies organized crime as a source of instability for society and associates critical infrastructures with it by exemplifying the actions of organized crime through attacks carried out in cyberspace related to critical infrastructures. In the same vein, Grabosky (2014, p. 1) analyses the term organized cybercrime in correlation with national security and believes that the latter is threatened by organized crime that makes use of cyber methods and means.

The Europol report (EU SOCTA 2021) identifies organized crime as a source of instability for society and associates critical infrastructures with it by exemplifying the actions of organized crime through attacks carried out in cyberspace related to critical infrastructures.

Zabyelina and Thachuk (2022, p. 1) analyse the relationship between the private sector and organized crime and consider that the latter is primarily a threat to the private sector, which also creates consequences for government organizations arguing that, by establishing monopolies over entire sectors, competitiveness within the economy is weakened and government tax collections are reduced.

CONCLUSIONS

Today's critical infrastructures were constructed approximately half a century ago, a time when security was not the primary concern for critical entities or public authorities. However, in the present day, man-made hazards such as hybrid threats, including terrorism and organized crime, pose significant challenges to the protection of these critical infrastructures.

Cyber vulnerabilities are poised to become the primary threat to critical infrastructures (Cockayne, Roth, 2017, p. 25). This is because individual data, such as online activity, medical device data, or network data from sectors like transportation or critical infrastructure will increasingly be automatically stored. This trend creates vulnerabilities related to theft, destruction, or ransom.

Thus, the protection of critical infrastructures is a serious and essential matter for all state actors and critical private entities responsible for providing essential services to the population. This issue cannot be addressed by a single policy or institution since

critical infrastructures are targeted by both terrorist organizations, planning and executing attacks for ideological, religious, or political reasons (Romanian Law no. 535/2004), and organized crime groups carrying out actions for financial gain.

BIBLIOGRAPHY:

1. Bennett, B.T. (2018). *Understanding, assessing, and responding to terrorism: Protecting critical infrastructure and personnel*. John Wiley & Sons.
2. Boin, A., SmitH, D. (2006). *Terrorism and critical infrastructures: Implications for public–private crisis management*. Public Money and Management 26.5, pp. 295-304.
3. Bologna, S., Lazari, Al., Mele, S (2015). *Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats*, pp. 79-90.
4. Bush, G.W. (February 2003). *The National Strategy to Secure Cyberspace.* The White House.
5. Chittester, C.G., Haimes, Y.Y. (2004). *Risks of terrorism to information technology and to critical interdependent infrastructures*. In Journal of Homeland Security and Emergency Management 1. 4.
6. Cockayne, J., Roth, A. (2017). *Crooked States: How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now.*
7. Council Framework Decision 2008/841/JHA, 24 October 2008 on the fight against organised crime. In *Official Journal of the European Union*, 300/42.
8. Frolov, K.V., Baecher, G.B. eds. (2006). *Protection of Civilian Infrastructure from Acts of Terrorism.* Vol. 12. Springer Science & Business Media.
9. Grabosky, P. (2014). *Organized crime and national security*. Korean Institute of Criminology Research Report Series, pp. 19-30.
10. Haimes, Y.Y., Longstaff, T. (2002). *The role of risk analysis in the protection of critical infrastructures against terrorism*. Risk Analysis 22.3, pp. 439-444.
11. *Romanian Law no. 535/2004 on preventing and combating terrorism*.
12. Lewis, J.A. (2002). *Assessing the risks of cyberterrorism, cyberwar and other cyberthreats.* Washington, DC: Center for Strategic & International Studies.

13. Marjanović, M., Nađ, I. (2013). *Assessment of threats to critical infrastructure facilities from serious and organized crime. National Critical Infrastructure Protection Regional Perspective.*
14. Mueller, J., Stewart, M.G. (2011). Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security. UK: Oxford University Press.
15. National Critical Infrastructure Security Liaison Officer's Handbook (2021). Ministry of Internal Affairs, Romania, CNCPIC.
16. Patterson, S.A., Apostolakis, G.E. (2007). *Identification of critical locations across multiple infrastructures for terrorist actions*. Reliability Engineering & System Safety 92.9, pp. 1183-1203.
17. Pătraşcu, P., Nicoară, G.F. (2023). *Adopting IoT Solutions for the Functionality, Protection and Resilience of Critical Infrastructures*. In *2023 17th International Conference on Engineering of Modern Electric Systems (EMES)*. IEEE.
18. Pîrjol, P., Chisega-Negrilă, A.-M. (2020). *Aspects regarding the use of passive sensors on air surveillance missions*. In "Carol I" National Defence Bulletin, 9.1, pp. 14-19.
19. Riedman, D., Warden, J., col. (2017). *The cold war on terrorism: Re-evaluating critical infrastructure facilities as targets for terrorist attacks*. Homeland Security Affairs 16, pp. 2-24.
20. Rudner, M. (2009). *Protecting Canada's critical national infrastructure from terrorism: mapping a proactive strategy for energy security.* In *International Journal* 64.3, pp. 775-797.
21. Shea, D.A., Resources, Science, and Industry Division (2003). *Critical infrastructure: Control systems and the terrorist threat.* Congressional Research Service, Library of Congress.
22. Stewart, M.G., Netherton, M.D., Rosowsky, D.V. (2006). *Terrorism risks and blast damage to built infrastructure*. In Natural Hazards Review 7.3, pp. 114-122.
23. Yao, X., Wei, H.H., Shohet, I.M., Skibniewski, M.J. (2020). *Assessment of terrorism risk to critical infrastructures: The case of a power-supply substation*. Applied Sciences, 10(20), p. 7162.
24. Wilson, C. (2014). *Cyber threats to critical information infrastructure.* Cyberterrorism: Understanding, Assessment, and Response. New York: Springer, pp. 123-136.

25. Zabyelina, Y., Thachuk, K.L., eds. (2022). *The Private Sector and Organized Crime: Criminal Entrepreneurship, Illicit Profits, and Private Sector Security Governance.* Taylor & Francis.
26. Zoli, C., Steinberg, L.J., Grabowski, M., Hermann, M. (2018). *Terrorist critical infrastructures, organizational capacity and security risk*. Safety Science, 110, pp. 121-130.