BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

The terrorist threat to critical infrastructure from the perspective of criminal risk

Sorina-Denisa POTCOVARU (DRAGNE), Ph.D. Candidate*
*Ministry of National Defence, Bucharest, Romania
e-mail: sorina.potcovaru@yahoo.com

Abstract

The field of critical infrastructure protection emerged as part of the fight against terrorism. Although a transition to an all-hazards approach has taken place, terrorism remains a significant threat to entities providing essential services. The relief of the legislative framework provides a nuanced understanding of the interrelationship between the constructs of critical infrastructure and terrorism, conceptualizing the latter in the context of criminal risk. By criminalizing acts of terrorism, the legislator intends to protect social values, including those values dependent on the functioning of critical infrastructure. Moreover, exemplification through case law contributes to identifying vulnerabilities and facilitates scenario building based on criminal risks.

Keywords:
critical infrastructure; critical infrastructure protection; terrorism; criminal risk.

Article info
Received: 2 November 2023; Revised: 29 November 2023; Accepted: 15 December 2023; Available online: 12 January 2024

Citation: Potcovaru (Dragne), S.D. 2023. "The terrorist threat to critical infrastructure from the perspective of criminal risk". *Bulletin of "Carol I" National Defence University*, 12(4): 239-252. https://doi.org/10.53477/2284-9378-23-62

The evolution of the European critical infrastructure protection system reflects a predominantly reactive stance by the European Union. Specific incidents, such as the terrorist attacks in Madrid (2004) and London (2006), were pivotal in prompting coordinated responses and legislative endeavors. These attacks underscored the vulnerability of critical infrastructures, prompting the European Union to broaden its policy, adopting an all-hazards approach that addresses a comprehensive spectrum of threats.

Within the legal framework, state interventions prioritize the protection of paramount societal relations and values. This is evident in the realm of criminal law, where legal norms safeguard sectors vital to society, including those linked to critical infrastructure. Human actions, whether through acts or omissions, emerge as a significant threat to this infrastructure. More often than not, these human behaviors are deemed unlawful, carrying legal repercussions. Among the legal ramifications, criminal liability stands out due to its association with actions of heightened societal risk. The potential of criminal acts targeting critical infrastructures, thereby jeopardizing the essential goods and services they deliver, accentuates the need to thoroughly examine criminal risk. This is imperative to fortify the defenses around critical infrastructure. Furthermore, the essence of criminal norms lies in the preservation of vital societal relations and values, including those intrinsic to the sectors of critical infrastructure.

Terrorism, within this context, is viewed as a unique expression of the broader criminal landscape. Its examination, concerning national and international security dimensions, requires a specialized approach rooted in criminal law methodologies. The aim of this article is to provide an examination of how terrorism, conceptualized as a criminal risk, impacts the security and functioning of critical infrastructures. Through this approach, the study aims to shed light on the vulnerabilities inherent within these infrastructures.

In this article, after general considerations about terrorism, as a threat to critical infrastructure, the legislative landscape of the terrorist phenomenon is outlined. The next section of the paper addresses terrorism from a legislative point of view in order to identify the implications at the level of critical infrastructure. The way in which jurisprudence serves as a source for identifying vulnerabilities to construct risk scenarios is exemplified through a case in which a person investigated for acts of terrorism fraudulently left the territory of Romania by exploiting vulnerabilities of port infrastructure.

The Terrorist Threat to Critical Infrastructure

The motivation of terrorist entities to attack critical infrastructures is built around the following considerations: "*critical infrastructures are targets of strategic value for society; by attacking them, the perpetrators can demonstrate the inability of state*

institutions to act, and the attacker has the opportunity to gain a high degree of publicity and notoriety" (INTERPOL 2018, 26). The implications of attacking critical infrastructures magnify the psychological repercussions.
Prevailing academic discourses underscore the necessity of aligning critical infrastructure protection strategies with societal values and anticipations (Burgess 2007). These values are protected at a cross-sectoral level by preventing and combating the effects of the destruction or disabling of critical infrastructure. Social values have a certain specificity at the sectoral level, especially where the legislator has recognized the need to protect certain areas of activity of particular social importance through criminal norms, corresponding to specific critical infrastructure sectors.
A deep dive into offenses, wherein critical infrastructures are posited as passive subjects, underpins the crux of this discourse. It emerges that both the criminal legislative apparatus and the specialized frameworks for critical infrastructure protection are anchored in upholding a constellation of societal values pivotal for state security. These values, intrinsic to the protection endeavors around critical infrastructures, are encapsulated in Directive 2022/2557, delineating "vital societal functions, economic activities, public health, and safety, or the environment" as the object of protection.

The frameworks provided by the UN and INTERPOL make a distinction between 'critical infrastructures' and 'soft targets', considering the classification of soft and hard targets. Soft targets, as per this classification, encompass areas marked by substantial human congregations - venues like shopping centers, recreational facilities, and religious establishments. Conversely, 'hard targets' denote sites that are heavily fortified and have limited access. An intersection exists between soft targets and critical infrastructures, highlighting a pivotal nuance. Even though the intrinsic value of soft targets might not always correlate with the provision of indispensable goods or services, it remains imperative to weave their protection into a cohesive strategy against terrorist threats (INTERPOL 2018, 22).
In the extensive compendium of best practices (INTERPOL 2018, 22), a detailed taxonomy concerning terrorist threats to critical infrastructures is presented. This taxonomy spans the ambit of hybrid threats. Delineated by the nature of these threats, a bifurcation emerges between physical threats and cyber threats. Taking the genesis of these threats into account, particularly the origin of the adversary, a distinction is drawn between internal and external threats. Additionally, these threats can be contextualized based on their targeted scope, ranging from individual entities to broader campaigns targeting multiple assets.

Societal implications regarding the regulation of the terrorist criminal phenomenon

The literature in the field has approached the nature of terrorism-related offenses. Such offenses are differentiated from other criminal activities by their distinct methods of

perpetration, which range from overt aggression to more covert, sophisticated tactics. The individuals behind these offenses often possess "a level of specialization, education, and cultural awareness that is both unique and extensive" (Cristescu 2004, 1).

It is imperative to contextualize the criminalization of terrorism within a specific branch of law. This is due to the unique attributes and multifaceted complexity of terrorism, as well as the pressing need to safeguard societal values through legal means, both domestically and internationally. Expert literature has already proposed the establishment of a branch of law dedicated to counterterrorism (Roach 2015, 3).

Counterterrorism law is characterized as a complex and challenging subject, typically falling under criminal law, a branch of public law, also "Counterterrorism law involves the interaction between the public and private sectors, particularly regarding the financing of terrorism and the telecommunications system" (Roach 2015, 3). Counterterrorism law intersects with constitutional law, as the fight against terrorism involves the limitation and restriction of fundamental human rights provided for in international treaties and the constitution of each country. For example, the activities of intelligence services, which are imperative in the fight against terrorism, impose certain limitations on the right to privacy.
Counterterrorism law represents a vast and complex field that encompasses norms from criminal, administrative, constitutional, and international trade law. It is one of the tools used by states and international communities in the fight against terrorism. Additionally, regulations regarding migration and the relationship between national and international law are also relevant.
The assassination of King Alexander I of Yugoslavia and French Foreign Minister Louis Barthou in Marseille in 1934 marked a turning point in acts of terrorism with international implications (Bararu 2010, 11). This incident brought the issue of terrorism to the attention of the League of Nations and led to the adoption of conventions in 1937.

The definition of terrorism from the second Conference on the Harmonization of Criminal Law in Brussels in 1930 is as follows: "Acts that involve the intentional use of means capable of endangering the common safety constitute acts of terrorism, which consist of crimes against life, liberty, and physical integrity of individuals or acts that are contrary to private or state property" (Bararu 2010, 11).
Subsequent amendments and evolutions have occurred, reflecting the dynamic nature of terrorism. Internationally, resolutions like the UN Security Council Resolution 1373 in 2001 and Resolution 2178 in 2014, alongside initiatives at the European Union level, have been instrumental in shaping the discourse.

A significant step in the criminalization of terrorism was the adoption of UN Security Council Resolution 1373 in 2001 (United Nations Security Council 2001), which calls on member states to ensure that terrorism and its financing are criminalized as serious offenses. The criminalization of terrorism and its financing as offenses is

one of the key instruments in the fight against terrorism, considering the preventive, educational, and corrective functions of criminal law. However, the resolution is criticized for not providing a universally accepted definition of terrorism.
In 2014, the UN Security Council adopted Resolution 2178 (United Nations Security Council 2014), which expands the scope of terrorism offenses, requiring states to criminalize and sanction acts related to the international travel of individuals for planning, organizing, and committing acts of terrorism.

Indeed, at the European Union level, the Council Framework Decision on Combating Terrorism was adopted in 2002, and it was later amended by another framework decision in 2008. This decision provides a taxonomy of the terrorist phenomenon within the European context, including "terrorist offenses, offenses related to a terrorist group, and offenses connected to terrorist activities" (Official Journal of the European Union 2002). These decisions have had a significant impact on the decisions and actions in the field of counterterrorism within the European Union.
Financing terrorism is indeed part of terrorist criminal activities and is internationally criminalized through the International Convention for the Suppression of the Financing of Terrorism (United Nation Organization 1999), adopted by the United Nations. The approach to criminalizing terrorist financing is similar in many states, with guidance provided by the Financial Action Task Force (FATF), an intergovernmental body established by the G7 countries. At the national level, countries have implemented their legislation to prevent and combat the use of the financial and banking system for terrorism financing purposes. In Romania, for example, Emergency Ordinance No. 159/2001 was adopted for the prevention and combating of the use of the financial and banking system for the financing of terrorist (Romanian Government 2001). Article 15 of this legislative act criminalizes the provision or collection of funds for the commission of terrorist acts.

Romania's journey in criminalizing terrorism can be traced back to its Penal Code of 1864, where "high treason" was first codified, as an offense against the internal and external security of the state. In the Penal Code of 1937, acts of terrorism were incriminated under the name of *crimes and offenses against the state*, and in post-war criminal legislation, the Penal Code of 1968 incriminated offenses against state security.
Despite robust legal frameworks, Romania has not been immune to terrorism, with several high-profile cases underscoring the persistent threat. These incidents, ranging from explosive attacks to propaganda and incitement, highlight the spectrum of challenges faced by law enforcement agencies (Roach 2015). In 2002, a Romanian citizen was accused of committing acts of terrorism and other offenses through a non-public decision of the High Court of Cassation and Justice. This individual had stolen multiple grenades and projectiles from a military depot, which were then thrown into the courtyard of a high school, resulting in casualties and damages. One year later, the same person attacked a heavily trafficked alley in the capital city with grenades.

In 2008, Romania encountered a case of propaganda for terrorist purposes. Through a website, the defendant promoted ideas and concepts specific to Islamic terrorist groups. Furthermore, they constructed an improvised explosive device intended for detonation in a public location. A threatening message announcing their intentions was sent to television stations. However, the defendant was apprehended before carrying out the attack.

The third case involves incitement to acts of terrorism. The defendant was accused of contacting another individual and persuading them to kidnap three Romanian journalists in Iraq. The purpose of this action was to exert pressure on policymakers regarding the withdrawal of military forces from the conflict zone (Roach 2015).

Legislative Analysis of Terrorism, implications for Critical Infrastructure

When examining the legal framework surrounding the criminalization of terrorism, the following perspectives have been identified for analyzing the implications in the field of critical infrastructures:

- Critical infrastructures as targets of terrorist offenses;
- The exploitation of these infrastructures in furthering terrorist agendas;
- The interplay at the institutional level between terrorism prevention and counterterrorism system and critical infrastructure protection system.

This importance arises from two main analytical streams: recognizing critical infrastructures as potential terrorist targets and understanding their role as passive subjects in terrorism-related offenses.

At the national level, Law No. 535/2004 stands as a pivotal legislative act in addressing acts of terrorism. Chapter V of the mentioned legislative act lists the offenses related to terrorism. The norm of criminalization is complex, considering that terrorism manifests itself through multiple offenses aimed at achieving the specific goals of terrorists or terrorist groups. Offenses already criminalized in the Penal Code, committed under the conditions of Article 1 of Law 535/2004, are adopted, but new offenses are also criminalized, which have no correspondence in other criminal laws and describe bioterrorism, nuclear terrorism, as well as the targeting of certain public utilities that correspond to critical infrastructures (Article 32, paragraph (3), letters c and e).

A closer perusal of Law 535/2005 underscores that the realm of terrorist targets encapsulates specific sectors of critical infrastructures. From the provisions of the two legislative systems, the correspondence emerges between the legal definition of material factors in Law 535/2004 and the sectors of the national critical infrastructure nominated by Government Emergency Ordinance no. 98/2010—which focuses on the identification, nomination, and safeguarding of critical infrastructures—draws attention to their concurrence, as depicted in Table 1.

TABLE 1 Materials Factors and Critical National Infrastructure

Material factors	*Sectors of Critical National Infrastructure*
Environmental factors	*Water, forests, and environment - Environmental protection*
Agricultural crops and livestock, food, and other consumer goods	*Food and agriculture*
Strategic objectives, military or with military utility	*National security*
Social infrastructure facilities	*Water, forests, and environment - Provision of drinking water and sewage* *Energy* *Financial and banking* *Healthcare*
State and governmental facilities	*Administration*
Transportation systems	*Transportation*
Telecommunications and information systems	*Information and communications technology*
National symbols and values	*Culture and national cultural heritage*

Critical infrastructures, when dysfunctional or destroyed, evoke societal repercussions reminiscent of those orchestrated by terrorist acts. Foundational to many definitions of terrorism is the utilization of violence to exert a profound psychological impact on the population. This profound effect is achievable when key infrastructure entities are targeted, taking into account the criteria for determining the *significant disruptive effect* regulated by Article 7 of Directive 2022/2557: users and other sectors and subsectors dependent on the essential services provided by the critical infrastructure, the degree and duration of the incident and the geographic area affected by the incident, the importance of the entity on the market including the availability of alternatives for the essential services (Official Journal of the European Union 2022). Those criteria can be used to quantify the effect of a terrorist attack.

From the content of the provisions of Law no. 535/2004, it follows that critical infrastructures can be targets of terrorist actions. The correspondence between the passive subjects of terrorism offenses and the sectors of the national critical infrastructure established by Government Emergency Ordinance no. 98/2010 is presented in Table no. 2.

TABLE 2 Critical infrastructure, targets of terrorist offenses

Transport Sector, *Air transport* subsector	Offenses regulated by the Aviation Code committed for specific terrorist purposes
Transport Sector, *Water transport* subsector *Energy* Sector (offshore oil platform)	Terrorism offenses committed on board or against a ship or fixed platform
Food and agriculture Sector	Infecting the atmosphere or water
Industry Sector *Information and communications technology* Sector *Food and agriculture* Sector	Acts of sabotage, as defined by article 403 of the Penal Code, committed for terrorist purposes
Energy Sector (nuclear) *Industry* Sector (nuclear and radioactive materials)	Non-compliance with the regime of nuclear materials and other radioactive substances

Additionally, Article 33, paragraph (2) of Law No. 535/2004 highlights potential infrastructural vulnerabilities which can be exploited by terrorists. These range from the physical security of the infrastructure to the classified information that could

assist in planning a terroristic act. To curtail the likelihood of pre-terroristic offenses, improvements in these sectors are imperative.

From the perspective of the terrorist threat, beyond enhancing the resilience of critical infrastructures to minimize the probability and impact of a terrorist attack, the capacity of well-protected infrastructures to prevent and act as deterrents and counter-terrorism factors can also be analyzed. In the literature, the concept of "weaponizing critical infrastructure" has been developed to describe the use of critical infrastructures as "instruments of warfare through their exploitation and obtaining strategic advantages by potential adversaries by attacking highly interconnected vital systems" (Evans 2020, 6).

Based on the analysis of legal provisions, it can be concluded, on one hand, how critical infrastructures can be weaponized and used as vectors of the terrorist phenomenon, and on the other hand, the contribution of well-protected and resilient infrastructures to the prevention and combatting of terrorism. The correlations are presented in Table no. 3.

TABLE 3 Critical infrastructure, vectors of the terrorist phenomenon

Information and Communications Technology Sector	prevention and combatting of incitement to terrorism through public incitement, or propaganda
Information and Communications Technology Sector	prevention and combatting of the phenomenon of radicalization through accessing and possessing terrorist propaganda materials
Financial-Banking Sector	prevention and combatting of terrorism financing offenses
Transport Sector *National Security* Sector, *Borders, Migration, and Asylum* subsector	prevention and combatting of cross-border movements for terrorist purposes
Energy Sector *Industry* Sector	prevention and combatting of the production or procurement of explosive devices, weapons, or hazardous substances

Thus, it follows that the criminal risk and, in particular, the terrorist risk must be an essential element in the risk analysis of critical infrastructures. This analysis needs to be materialized in the Security Plan of the operator, taking into consideration the following two perspectives:

- Critical infrastructures as potential targets of terrorist attacks;
- Critical infrastructures as possible vectors of the terrorist phenomenon.

Therefore, adapted protection measures are necessary concerning the specific construct of terrorism to prevent or limit the effects generated by possible destruction or impairment of critical infrastructure elements in a terrorist attack. Considering the highly interconnected nature of infrastructure systems, they can be analyzed as direct or indirect targets of terrorist attacks, and the indirect effects that spread along the network of dependencies and interdependencies are also significant. Moreover, it is essential to identify vulnerabilities that allow the exploitation of infrastructure elements for terrorist purposes, considering the integration of critical infrastructure protection

into the extensive process of enhancing society's resilience against the terrorist threat.
Given the identified correspondences, critical infrastructures need to be approached as potential targets of terrorist activities, and it is opportune to combine institutional efforts aimed at preventing and combating terrorism with the protection of critical infrastructures where these two domains intersect. Furthermore, the majority of institutions that are part of the National System for Preventing and Combating Terrorism are also responsible public authorities represented in the Interinstitutional Working Group for the Protection of Critical Infrastructures.
Law No. 535/2004 on the prevention and combatting of terrorism was amended and supplemented by Law No. 58/2019 to transpose the provisions of Directive 2017/541 of the European Parliament and the Council of the European Union on combating terrorism. According to the 2019 Activity Report of DIICOT, the legislative amendment reflects "internal and international developments related to the terrorist phenomenon, institutional changes, and the national security objectives of Romania" (DIICOT 2020). Moreover, the changes brought by Law No. 58/2019 enable better cooperation among the authorities within the NSPCI, as well as between them and external partners.

For a systemic approach to critical infrastructure and the generation of relevant protection measures against terrorist threats, an institutional analysis is necessary regarding the cooperation between responsible public authorities and the National System for Preventing and Combating Terrorism (NTPCS).
By comparing the list of responsible public authorities approved by Government Decision No. 35/2019 and the composition of the National Terrorism Prevention and Counterterrorism System. (NTPCS) provided in Law No. 535/2004, the following responsible public authorities are not part of the NSPCT:

- Ministry of Energy;
- National Sanitary Veterinary and Food Safety Authority;
- Ministry of Research and Innovation;
- Romanian Space Agency;
- Ministry of Culture and National Identity.

It can be observed that all Critical National Infrastructure (CNI) sectors are represented in the NTPCS by at least one responsible public authority, except for the Culture and National Cultural Heritage sector. As indicated in the specialized literature, the motivation behind terrorist attacks is often religious and ideological. Therefore, the cultural component is an important element in the analysis of the terrorist criminal risk toward critical infrastructures. The legitimacy of cultural attacks throughout history, as well as the status of cultural institutions as symbolic infrastructures, possible targets of terrorist entities, are arguments for the inclusion of the Ministry of Culture and National Identity in the NTPCS to enhance the protection of critical cultural infrastructures from a terrorist threat perspective.
Furthermore, considering the threat posed by nuclear terrorism and the strategic nature of critical energy infrastructure elements, the Ministry of Energy must be included in the NTPCS as well.

Exemplification of how vulnerabilities in critical infrastructure are exploited for the committing terrorist offenses

This section evaluates the vulnerabilities of critical infrastructure in the context of terrorist activities. By employing Decision No. 309/A/2014 of the High Court of Cassation and Justice, Penal Section as the primary dataset, this research elucidates how legal outcomes can offer significant insights into the modus operandi of criminals, thereby assisting in constructing informed threat scenarios. Analyzing a crime, underpinned by a juridical verdict, provides a structured framework to understand infrastructure vulnerabilities and build realistic threat scenarios.
The central document for this investigation is Decision No. 309/A/2014, wherein three individuals were adjudicated for abetting fraudulent border crossing of a suspect under terror activity investigation. The investigation ongoing was linked to the kidnapping of Romanian journalists in Iraq, a case that garnered widespread media attention, both nationally and internationally. This case encompasses two primary narrative trajectories: firstly, the orchestration and financing of a terror act, and secondly, the aiding of a suspect in illicitly exiting Romania, classified as a terror offense as per prevailing statutes.
The analytical focus is placed on the crime of aiding departure from the national territory of Omar Hayssam, offering a lens into transport infrastructure susceptibilities, especially those of ports.

In Southeastern Romania, the Port of Constanta is a significant infrastructure site, as evidenced by its involvement in the Omar Hayssam case. The court statement outlined Hayssam's evasion strategy, noting its sophistication and the influence of manipulated media narratives. Such findings indicate the essential role of transport operators that activate at the level of critical infrastructure in security assessments, highlighting potential threats and the occasional concealment of illicit actions via corporate facades (High Court of Cassation and Justice 2014).
From the point of view of Critical Infrastructure analysis, judicial findings corroborate that criminals strategized around infrastructure vulnerabilities. The fact that the modus operandi of the criminals was built around exploiting the vulnerabilities of the infrastructure is also confirmed by the court: "The decision regarding the chosen route was based on the obtained information regarding the vulnerability of the border area represented by the Port of Constanta, aspects that were observed during the investigations conducted in the present case" (High Court of Cassation and Justice 2014).

It follows that transport operators engaging in activities related to critical infrastructure and operating within the area of interest and influence of the critical entity must be included in the security environment analysis of the Critical Infrastructure Network (CIN) and treated as potential sources of threats within the risk analysis. In many cases, offenders camouflage their illicit activities through the companies they administer or control.

The analysis report of the Organized Crime Combat Brigade Constanța, reconstructed within the judicial decision pronounced in the case of Omar Hayssam (Decision No. 309/A/2014 of the High Court of Cassation and Justice), identifies a series of vulnerabilities in the port infrastructure regarding the transportation of clandestine passengers. According to this report, "boarding a commercial vessel docked at the ports of Constanta, Constanța Sud Agigea, and Midia can be performed by any person somewhat familiar with port traffic, without requiring prior activities or concealment maneuvers" (High Court of Cassation and Justice 2014). Thus, in 2006, the port infrastructure in Constanța presented the following vulnerabilities:

- Absence of a robust access control system.
- Boarding can be performed with only the permission or complicity of the ship captain.
- Numerous unmonitored hiding spots within ships.
- Limited video surveillance.
- Subpar security protocols, relying heavily on barriers and non-standardized security personnel.

Moreover, significant relations between the defendant and border authorities reveal vulnerabilities within the National Critical Infrastructure's human component. Thus, the human vulnerability of these critical infrastructures is identified, where employees have connections to criminal environments and can be influenced to misuse their public authority prerogatives.
Considering the vulnerabilities identified within the analyzed infrastructure, measures for enhancing protection can be identified and developed, ranging from physical protection of critical infrastructure assets to training and ethics of personnel.

Expanding upon the discussions, it is imperative to consider the broader ramifications associated with the potentiality of a nuclear incident or attack. Naval transport means, such as the vessel used by Omar Hayssam, and the control systems at existing border crossing points, present real vulnerabilities in terms of a potential terrorist or even nuclear attack. The transport and border infrastructure could facilitate the transportation of nuclear materials by terrorist entities. The existence of scanning devices on ships, capable of detecting the unique signature emitted by nuclear materials and thermal imaging for person detection, would significantly enhance the protection of critical infrastructures and significantly reduce the risk of illegal movements by terrorists and nuclear materials.

The threat of a nuclear attack is significant for the port infrastructure in Constanța, with the main vulnerability lying in the container transport system. The hypothesis of nuclear material or weapons and devices being transported within the European Union should also be taken into account. These could be transported by road along pan-European routes, by rail, but most likely by sea, exploiting the vulnerabilities associated with container transport. Air transport is unlikely due to heightened security measures in this sector.

One of the specific vulnerabilities of port infrastructure is the insecurity of containers in terms of the goods they can carry, as well as the existence of access control systems for people and goods that do not meet the technical requirements concerning the threat posed by the clandestine transport of nuclear materials.

Taking into consideration the case analyzed in this section, in Romania, especially in the area of the Constanța port, the following possible courses of action can be used for risk scenario building:

- Illegal procurement of raw materials and theft of sensitive technical information from a nuclear power plant, taking Cernavodă Power Plant as an example;
- Romania serves as a transit country for the illegal transportation of nuclear materials and devices, especially through maritime containers. Although this action may not result in an explosion on Romanian or neighboring states' territory, it creates a state of danger considering that this type of transport requires special security measures that are not implemented for clandestine transportation;
- Execution of a nuclear attack on Romanian territory. Although Romania has not been a direct target of international terrorist attacks so far, this course of action deserves consideration because it represents an incident with a low probability but significant impact.

Case law serves as a pivotal tool, offering profound insights into criminal modus operandi and causality based on which vulnerabilities and protection measures are identified. The examination of Hayssam's evasion illuminates the vulnerabilities inherent within transport infrastructures like the Constanța port. Consequently, judicious evaluations stand as invaluable assets in understanding criminal risks and in the framing of holistic threat scenarios for critical infrastructures.

Proposals

The interplay between terrorism risks and critical infrastructure underscores the indispensable importance of their examination within the realms of both national and international security frameworks. An act of terrorism targeting such infrastructures could culminate in devastating societal impacts, further exacerbated by the intricate interdependencies that characterize the critical infrastructure system. This interaction can be integrated into the risk analysis of critical infrastructures for comprehensive protection.

Critical infrastructures, owing to their societal significance, are not only susceptible to terrorist activities but can also potentially serve as conduits for these acts. Moreover, the analysis of the legal documents elucidates the legislative recognition of this intertwined relationship. Even if it is not a direct threat to critical infrastructure,

this perspective must be addressed in the extended context of resilience because critical infrastructure exploited for terrorist activities represents just an entry point for targeting the entire society.

Interinstitutional cooperation represents one of the necessary measures to enhance the protection of critical infrastructures regarding the terrorist threat. Despite the establishment of legislative and institutional systems at the national level for protecting critical infrastructures, as well as for preventing and combating terrorism, clear gaps remain, especially regarding the representation of key sectors within the National System for Preventing and Combating Terrorism.

The confluence of values preserved by criminal laws addressing terrorism's criminalization aligns succinctly with the values articulated within the legal characterization of critical infrastructure, as stipulated in Article 2, point 5 of Directive 2022/2557. Consequently, counter-terrorism initiatives emerge as inherent components of the overarching strategy for critical infrastructure protection. Such strategies must be adaptive, anticipating and addressing the multifaceted and evolving modi operandi of terrorist entities. Embracing a proactive stance by viewing critical infrastructures as potential terrorist targets facilitates a systematic vulnerability assessment, drawing parallels between terrorists' operational tactics and potential risk scenarios.

From a methodological point of view, the analysis of the legislative framework constructed around the main concepts of the research: *terrorism* and *critical infrastructure* highlights intricate correlations between these two domains and presents new research directions and perspectives regarding critical infrastructures and their protection against terrorist threats.

Moreover, jurisprudence proves to be a valuable source for illustrating cases in which critical infrastructure objectives are implicated in the commission of a terrorist offense, either as targets of attacks or as vectors for the manifestation of criminal activity by exploiting vulnerabilities. Hence, beyond identifying vulnerabilities, these jurisprudence-based case studies form the foundation for developing potential risk scenarios, serving as highly useful tools in the planning and enhancement of critical infrastructure protection.

Concluding, the dynamic nature of terrorism and its evolving methodologies necessitate an equally adaptive approach to critical infrastructure defense. Continued collaboration among public authorities, the enhancement of legislative provisions, and bolstered public-private partnerships can enhance the resilience of critical infrastructure.

References

Bararu, Iosif. 2010. *Infracțiunile de terorism. Legislație și procedură penală*. București: Universul Juridic.

Burgess, J.P. 2007. „Social Values and Material Threat: The European Programme for Critical Infrastructure Protection." *International Journal of Critical Infrastructures* 3 (3-4): 471-487.

Cristescu, Doru Ioan. 2004. *Criminalistic and Judicial Investigation of Offenses against National Security and Terrorism.* Timişoara: Solness Publishing.

DIICOT. 2020. „Activity Report 2019." Bucharest. https://www.diicot.ro/informatii-de-interes-public/raport-de-activitate.

Evans, C.V. 2020. „Future Warfare: Weaponizing Critical Infrastructure ." *The US Army War College Quarterly: Parameters* 50 (2): 6.

High Court of Cassation and Justice. 2014. „Decision No. 309/A/2014." https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=121153.

INTERPOL. 2018. „The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium of Good Practices." Compiled by CTED and UNOCT. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.

Official Journal of the European Union. 2002. „Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)." Series L, No. 164, June 22.

__. 2022. „Directive (EU) 2022/2557 of the European Parliament and of the Council of December 14, 2022, on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC." L333/164, December 27, 2022.

Roach, Kent. 2015. *Comparative Counter-Terrorism Law.* Cambridge: Cambridge University Press.

Romanian Government. 2001. „Emergency Ordinance No. 159 of November 27, 2001, for the Prevention and Combating of the Use of the Financial-Banking System for the Purpose of Financing Acts of Terrorism." Published in the Official Gazette of Romania, No. 802, December 14, 2001.

__. 2010. „Emergency Ordinance No. 98/2010 on the Identification, Designation, and Protection of Critical Infrastructures." Published in the Official Gazette, No. 757, November 12, 2010.

Romanian Parliament. 2004. „Law No. 535/2004 on the Prevention and Combating of Terrorism." Published in the Official Gazette, No. 1161, December 8, 2004.

United Nation Organization. 1999. „International Convention for the Suppression of the Financing of Terrorism." Published in the Official Gazette of Romania, No. 852, November 26, 2002.

United Nations Security Council. 2001. Resolution 1373 (September 28, 2001), New York.

__. 2014. Resolution 2178 (September 24, 2014), New York.