BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

From Targets to Tools: the Complex Relationship between Critical Infrastructures and Hybrid Threats

Sorina-Denisa POTCOVARU (DRAGNE), PhD Candidate*
Professor Marinel-Adi MUSTAȚĂ, PhD**

*Interdisciplinary Doctoral School, "Carol I" National Defence University, Bucharest, Romania
e-mail: sorina.potcovaru@yahoo.com
**Faculty of Security and Defence, "Carol I" National Defence University, Bucharest, Romania
e-mail: mustata.adi@unap.ro

Abstract

The complexity of the interaction between critical infrastructures and hybrid threats emerges in the specialized literature through a diversity of perspectives and approaches. This study investigates how the two concepts intersect, highlighting hybrid manifestations that combine cyberattacks, disinformation campaigns, kinetic operations, economic coercion, and the exploitation of legal grey zones in international law. At the same time, critical infrastructures are analyzed both as strategic targets and as instruments for the propagation of hybrid threats, being weaponized through the exploitation of their sectoral and inter-sectoral vulnerabilities, and thus generating cascading effects. Examples from the literature highlight not only the cyber and economic dimensions of such hybrid actions but also the difficulties of attribution and the multidimensional nature of the typology of the actors involved. The conclusions of the article emphasize the necessity of understanding hybrid threats and critical infrastructures as interconnected realities, whose protection and resilience require a systemic and coordinated approach, capable of responding to the complex challenges of contemporary security.

Keywords:
Hybrid Threats; Critical Infrastructures; Interdependencies; Cyberattacks; Disinformation; Economic Coercion; Weaponizing; Resilience.

Article info
Received: 1 August 2025; Revised: 2 September 2025; Accepted: 15 September 2025; Available online: 6 October 2025

Citation: Potcovaru (Dragne), S.D., and M.A. Mustață. 2025. "From Targets to Tools: the Complex Relationship between Critical Infrastructures and Hybrid Threats." *Bulletin of "Carol I" National Defence University*, 14(3): 318-327. https://doi.org/10.53477/2284-9378-25-51

The transformations of the international security environment have brought hybrid threats to the forefront, defined by the combination of conventional and unconventional, military and non-military means, employed to exploit the vulnerabilities of states and international organizations with the purpose of destabilizing democratic societies to the advantage of hostile state and non-state actors. In this context, critical infrastructures occupy a central position, both through their essential role in ensuring the functioning of modern societies and through their high degree of interdependence and exposure to complex attacks.

The literature emphasizes that critical infrastructures are simultaneously strategic targets and channels for the propagation of hybrid threat vectors within democratic societies. Cyberattacks, disinformation campaigns, kinetic operations, economic coercion, as well as actions conducted in "grey zones," represent the main modalities through which state and non-state actors exploit these vulnerabilities. At the same time, the concept of critical infrastructure is approached in the literature from multiple perspectives, general, sectoral, and inter-sectoral, reflecting the diversity of analytical frameworks and understandings of the phenomenon.

This study aims to analyze the manifestation of hybrid threats against critical infrastructures, drawing on three major directions identified in the literature: (1) the conceptualization of critical infrastructures, from general to sectoral approaches; (2) the conceptualization and operationalization of hybrid threats; and (3) the relationship between critical infrastructures and hybrid threats. This structure allows for the highlighting of the complexity of the phenomenon and the outline of a comprehensive picture of the current challenges to the resilience of critical infrastructures in the face of hybrid threats.

The present article is based on an analysis of the literature addressing the manifestation of hybrid threats against critical infrastructures. The literature includes scientific articles indexed in the Web of Science database (n=8) and research reports (n=10) developed under the auspices of the European Union, the North Atlantic Treaty Organization, and the European Centre of Excellence for Countering Hybrid Threats.

Critical Infrastructures, from General to Sectoral

The analysis of the specialized literature reveals that critical infrastructure is conceptualized differently depending on the degree of specificity adopted by researchers. Thus, three main directions can be distinguished: a general approach, which addresses critical infrastructure as a whole; an inter-sectoral approach, focused on the interdependencies between sectors; and a sectoral approach, oriented toward the vulnerabilities of a particular domain.
Studies adopting a general approach start from the premise that critical infrastructures, in their entirety, constitute strategic objectives for actors employing

instruments specific to hybrid threats. In this direction, Boyte (2017) highlights how cyberattacks can simultaneously affect government services, financial networks, and telecommunications systems, thereby generating systemic instability. In the same line, Mazaraki and Goncharova (2022) emphasize that digital interconnectivity facilitates the conduct of hybrid attacks in the legal "grey zone." Jukka (2019) also stresses the dependence of critical infrastructures on digital networks, which amplifies their exposure to hybrid threats. A complementary perspective is offered by Wigell, Mikkola, and Juntunen (2021), who argue for the necessity of a whole-of-society strategy to protect infrastructures in the context of cumulative effects produced by hybrid attacks targeting multiple sectors simultaneously. Conceptually, Giannopoulos, Smith, and Theocharidou (2021) integrate infrastructure into the general model of hybrid threats, treating it as a key domain of action.

Literature further underscores the interdependencies among infrastructures, identifying them as significant sources of vulnerability when confronted with hybrid threats. Aho, Midoes, and Šnore (2020) show how financial infrastructure becomes exposed due to its connections with the energy and telecommunications sectors. Similarly, Carlsson and Gustavsson (2017) analyze the dependence of the energy infrastructure on the telecommunications sector, identifying it as a vulnerability exploitable by hostile actors.

Fiott and Parkes (2019) underscore the central role of digital infrastructure, indispensable for the functioning of both civilian and military infrastructures, while also serving as a potential entry point for inter-sectoral attacks. Tessari and Muti (2021) focus on the interdependence between energy and telecommunications infrastructures, arguing that destabilization in these areas can simultaneously affect both national economies and defense capabilities. Nave et al. (2022) discuss inter-sectoral vulnerabilities between energy and transport infrastructures, particularly in the context of NATO cooperation in the Baltic Sea region. Similarly, Bueger and Liebetrau (2021) highlight the importance of submarine communication cables, on which critical domains such as telecommunications, finance, and defense depend.

Another direction explored in the literature concerns the focus on specific types of infrastructure. The Hybrid CoE report (2019) examines nuclear energy infrastructure as a strategic target for hybrid actors, given its dual-use applications in both civilian and military domains. Evans (2020) reaches a similar conclusion regarding energy networks, stressing the significant impact that a hybrid attack could have on both civilian and defense sectors.

Concerning communications infrastructure, Jokinen, Normark, and Fredholm (2022) analyze vulnerabilities that can be exploited by non-state actors. Maritime infrastructure is also a prominent target: Schaub, Murphy, and Hoffman (2017) demonstrate how ports and maritime communication lines can be attacked to disrupt global trade and military logistics. Jukka et al. (2019) emphasize the specific

vulnerabilities of submarine cables and maritime routes located in geopolitically sensitive regions. Along the same lines, Bueger et al. (2022) underline the dual-use character of submarine cables, which are essential for both civilian and military communications. Finally, Demertzis and Wolff (2020) examine the financial sector, pointing out weaknesses such as fragmented security and the excessive centralization of payment systems, banking structures, and insurance markets.

The three approaches, general, inter-sectoral, and sectoral, provide a complex picture of how critical infrastructure is analyzed in the context of hybrid threats. Although the approaches differ, a common theme emerges: interconnectivity. Whether analyzed at the macro, inter-sectoral, or sectoral level, the dependence between systems constitutes a fundamental source of vulnerability that hybrid actors exploit to generate effects with systemic impact.

The Operationalization of Hybrid Threats in Relation to Critical Infrastructures

The specialized literature addresses hybrid threats through a variety of concepts and modes of operation, with a common focus on exploiting the vulnerabilities of critical infrastructures. The analysis of studies reveals several recurring thematic directions: the centrality of the cyber dimension, the use of disinformation, the conduct of kinetic operations, economic coercion, the exploitation of grey zones, and issues of non-attribution. In parallel, the literature also examines the typology of actors involved, both state and non-state, and the relationships between them.

The cyber dimension consistently emerges as a central element of hybrid threats, particularly in connection with attacks on critical infrastructures. Boyte (2017) provides a comparative analysis of cyberattacks conducted by Russia-sponsored actors against financial, governmental, and telecommunications infrastructures in Estonia, the United States, and Ukraine. A distinctive feature of these operations is their execution in the digital "grey zone," where the difficulty of attribution complicates state responses (Mazaraki and Goncharova 2022). Carlsson and Gustavsson (2017) demonstrate the effectiveness of attacks on energy infrastructures, highlighting their dependency on digital networks. Other studies (Jukka 2019; Evans 2020) emphasize the vulnerabilities of dual-use infrastructures (civilian and military), especially in the energy and communications sectors.

The financial sector is likewise a privileged target: Aho, Midoes, and Šnore (2020) investigate how cyber espionage exploits vulnerabilities in payment systems, while Demertzis and Wolff (2020) note the intensification of cyberattacks against banks and stock exchanges, with the involvement of non-state actors.

Disinformation campaigns appear as amplifiers of the effects of hybrid threats on critical infrastructures. Wigell, Mikkola, and Juntunen (2021) argue that by

influencing public opinion, such campaigns can delay governmental responses. Tessari and Muti (2021) illustrate the synergy between disinformation and cyberattacks in the context of Europe's energy dependence on Russia. In the maritime sector, disinformation targets the security of ports and trade routes, generating economic insecurity (Schaub, Murphy and Hoffman 2017), while disinformation campaigns concerning submarine cables amplify the effects of both physical and cyberattacks (Bueger and Liebetrau 2021). Demertzis and Wolff (2020) further underline the combined impact of disinformation and social engineering in undermining public trust in financial institutions.

Hybrid threats also include physical components, complementing cyber operations. Examples include the sabotage of ports and submarine cables (Schaub, Murphy and Hoffman 2017; Bueger and Liebetrau 2021). Bueger et al. (2022) highlight the role of non-state actors, supported by Russia and China, in physical attacks against submarine cables, combined with cyber operations and the use of underwater drones. Moreover, nuclear energy infrastructure is an especially sensitive target, where hybrid attacks could generate major environmental and security consequences (Hybrid CoE 2019).

Economic coercion is analyzed as a specific instrument of state actors. Evans (2020) shows how China uses foreign direct investment to gain control over energy and telecommunications infrastructures. Fiott and Parkes (2019) discuss the vulnerability of the European Union's financial system to economic manipulation by external actors.

A key feature of hybrid threats is their conduct in "grey zones" and the challenge of attribution. Cyberattacks on infrastructures are often non-attributable (Mazaraki and Goncharova 2022), allowing hostile actors to exploit the time gained to carry out further actions (Hybrid CoE 2019). Jokinen, Normark, and Fredholm (2022) argue that non-state actors can function as state proxies, exploiting the lack of a well-defined legal framework. Similarly, Nave et al. (2022) underscore the persistence of legal ambiguity in the Baltic region, where both cyberattacks and acts of physical sabotage continue to resist clear legal categorization.
In most studies, Russia and China are identified as central state actors. Russia employs cyberattacks (Fiott and Parkes 2019; Boyte 2017), exploits infrastructural interdependencies (Jukka 2019), and applies energy pressures on Europe (Tessari and Muti 2021). China is analyzed in relation to cyberattacks against nuclear infrastructures (Hybrid CoE 2019) and its use of economic control through investment (Evans 2020).

Non-state actors include hacktivists and cyber mercenaries (Carlsson and Gustavsson 2017; Mazaraki and Goncharova 2022), as well as pirates or terrorist networks targeting maritime infrastructure (Bueger and Liebetrau 2021; Jukka, et al. 2019). In some cases, they collaborate with states, acting as proxies or auxiliaries (Evans 2020; Tessari and Muti 2021). Jokinen, Normark, and Fredholm (2022)

propose a detailed taxonomy, classifying non-state actors as proxies, auxiliaries, or surrogates, depending on their relationship with states.

The analysis of the literature confirms the multidimensional character of hybrid threats. Cyberattacks are recurrent and central, kinetic operations complement digital actions, disinformation amplifies effects, while the economic dimension and exploitation of grey zones reinforce the effectiveness of these tactics. Furthermore, the interaction between state and non-state actors makes it particularly difficult to identify perpetrators and to design effective response strategies.

The Relationship between Critical Infrastructures and Hybrid Threats

The specialized literature highlights a close connection between critical infrastructures and the manifestation of hybrid threats through an interconnected approach to these two concepts. The analysis of studies reveals three main thematic directions: critical infrastructures as targets, their use as weapons (weaponizing), and the exploitation of the economic and social vulnerabilities associated with them.

The vital nature of critical infrastructures makes them prime objectives for hybrid actors. Boyte (2017) shows that the cyberattacks carried out in Estonia, the United States, and Ukraine targeted infrastructures such as telecommunications, governmental services, and financial systems, with the aim of destabilizing state functions. In a similar analysis, Jukka (2019) underscores the systemic importance of infrastructures, noting that their interdependencies amplify the cascading effects generated when a single sector is attacked.

An additional source of vulnerability lies in the dual-use nature of critical infrastructures. Energy and communications networks, with both civilian and military applications, become strategic targets, affecting society and defense capabilities simultaneously (Evans 2020). Nuclear infrastructure is especially sensitive due to its potential for major impacts on both security and the environment (Hybrid CoE 2019).

Another thematic trend identified is the use of infrastructures not only as targets but also as instruments of hybrid threats. Evans (2020) defines weaponizing critical infrastructure as a long-term strategy aimed not merely at causing immediate disruptions but at undermining national security and defense capabilities. He provides examples of how Russia, China, Iran, and North Korea apply this strategy against energy, transport, telecommunications, and defense industry infrastructures, particularly targeting the United States and NATO member states.

Carlsson and Gustavsson (2017) further show that cyberattacks on energy infrastructures can force governments to allocate significant resources to restoring

services, diverting attention from a strategic response. The Coherent Resilience Baltic 2021 exercise illustrates how energy can be transformed into a tool for destabilizing regional cooperation and military alliances (Nave, et al. 2022). Similarly, the vulnerabilities of submarine cables are exploited to disrupt dependent infrastructures such as communications, financial systems, or even military operations.

The third thematic direction highlights how hybrid actors exploit the economic and social weaknesses associated with critical infrastructures. Russia, for instance, manipulates energy supply chains to create dependency and exert economic coercion in pursuit of geopolitical objectives (Tessari and Muti 2021). Similarly, financial infrastructure is exploited through tactics of coercion and manipulation: Aho, Midoes, and Šnore (2020) show how it can be destabilized by hybrid attacks, while Fiott and Parkes (2019) discuss external pressures designed to weaken the financial system of the European Union. Maritime infrastructure is also targeted to exploit the global dependence on trade, thereby generating economic and strategic instability at the international level.

Overall, the relationship between critical infrastructures and hybrid threats is characterized by a dual dimension: critical infrastructures are simultaneously targets and instruments. Interdependence, dual-use characteristics, and economic and social vulnerabilities increase the attractiveness of infrastructures for hybrid actors. This reality reinforces the argument that the protection of critical infrastructures must be addressed through a systemic and multidimensional approach.

Conclusions

The analysis of the specialized literature confirms that the relationship between critical infrastructures and hybrid threats is complex, multidimensional, and evolving. From a conceptual perspective, critical infrastructures are addressed in general terms as an interconnected system essential for the functioning of modern societies, as well as sectorally or inter-sectorally, depending on the specific vulnerabilities of each domain. This diversity reflects the recognition of the central role of infrastructures in the equation of contemporary security.

Hybrid threats manifest through a wide spectrum of actions, with the cyber dimension recurrent and dominant, complemented by disinformation, kinetic operations, and economic coercion. The exploitation of "grey zones" and the difficulty of attribution enhance the effectiveness of these actions, granting hostile actors the freedom to operate below the threshold of conventional armed conflict. Moreover, the interaction between state and non-state actors reinforces the challenging nature of countering such threats.

The relationship between critical infrastructures and hybrid threats can be approached through a dual dimension: critical infrastructures simultaneously

represent targets of hostile actions and instruments employed for the destabilization of states and alliances. Interdependence, dual-use characteristics, and economic and social vulnerabilities increase the attractiveness of infrastructures for hybrid actors, generating cascading effects at national, regional, and global levels.

Considering the analysis conducted, it becomes clear that critical infrastructures can no longer be regarded solely as vulnerable targets of hybrid threats but also as strategic instruments transformed and instrumentalized by hostile actors to generate destabilizing effects across multiple levels. This dual stance, of infrastructures as both objectives and weapons, illustrates the complexity of the phenomenon and highlights the interconnectedness of the two key concepts. Consequently, understanding the relationship between critical infrastructures and hybrid threats requires moving beyond a sectoral vision toward a systemic and integrated perspective, one that captures the dynamics through which vulnerability can be transformed into a lever of pressure and destabilization.
It follows that the protection of critical infrastructure in European democratic societies requires a systemic, multidimensional, and integrated approach that combines technological resilience, inter-institutional cooperation, and international coordination.

Furthermore, future research directions should capture the complexity of the phenomenon and promote the integration of sectoral approaches developed at NATO and the European Union levels. Future studies should investigate coordination mechanisms between these two organizations, explore inter-sectoral scenarios, and develop analytical tools capable of integrating the cyber, economic, informational, and legal dimensions of hybrid threats.

Only through such mechanisms can the destabilizing impact of hybrid threats be limited and the response capacities of states and democratic organizations be strengthened. The need for a systemic approach to the resilience of critical infrastructures derives from the structural interdependence of these systems and from the multidimensional character of hybrid threats.

References

Aho, Aleksi, Catarina Midões, and Arnis Šnore. 2020. *Hybrid Threats in the Financial System*. Hybrid CoE Working Paper 8. The European Centre of Excellence for Countering Hybrid Threats.

Boyte, Kenneth J. 2017. "A Comparative Analysis of the Cyberattacks Against Estonia, the United States and Ukraine." *International Journal of Cyber Warfare and Terrorism* 7(2): 1–15. https://doi.org/10.4018/ijcwt.2017040104.

Bueger, Christian, and Tobias Liebetrau. 2021. "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network." *Contemporary Security Policy* 42(4): 590–616. https://doi.org/10.1080/13523260.2021.1907129.

Bueger, Christian, Tobias Liebetrau, and Jonas Franken. 2022. *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Carlsson, Anders, and Rune Gustavsson. 2017. "The Art of War in the Cyber World." In *2017 4th International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, 453–456. https://doi.org/10.1109/INFOCOMMST.2017.8246345.

Demertzis, Maria, and Guntram Wolff. 2020. "Hybrid and Cyber Security Threats and the EU's Financial System." *Journal of Financial Regulation* 6(2): 180–201. https://doi.org/10.1093/jfr/fjaa006.

Evans, Carol V. 2020. "Future Warfare: Weaponizing Critical Infrastructure." *Parameters* 50(4): 59–70. https://doi.org/10.55540/0031-1723.1017.

Fiott, Daniel, and Roderick Parkes. 2019. *Protecting Europe: The EU's Response to Hybrid Threats*. Luxembourg: Publications Office of the European Union.

Giannopoulos, Georgios, Hanna Smith, and Marianthi Theocharidou. 2021. *The Landscape of Hybrid Threats: A Conceptual Model: Public Version*. Hybrid CoE Research Report. Luxembourg: Publications Office of the European Union.

Hybrid CoE. 2019. *Nuclear Energy and the Current Security Environment in the Era of Hybrid Threats*. Hybrid CoE Research Report. The European Centre of Excellence for Countering Hybrid Threats.

Jokinen, Janne, Magnus Normark, and Michael Fredholm. 2022. *Hybrid Threats from Non-State Actors: A Taxonomy*. Hybrid CoE Research Report 6. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen. 2019. *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?* Hybrid CoE Working Paper 4. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen, Terry Gill, Valentin Schatz, Lauri Ojala, Tadas Jakštas, and Pirjo Kleemola-Juntunen. 2019. *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans*. Hybrid CoE Working Paper 5. The European Centre of Excellence for Countering Hybrid Threats.

Mazaraki, Nataliia, and Yulia Goncharova. 2022. "Cyber Dimension of Hybrid Wars: Escaping a 'Grey Zone' of International Law to Address Economic Damages." *Baltic Journal of Economic Studies* 8(2): 115–120. https://doi.org/10.30525/2256-0742/2022-8-2-115-120.

Nave, C., V. Kopustinskas, E. Dirginčius, L. Walzer, G. Beniulytė, A. Purvins, M. Masera, D. Nussbaum, V. Norg, and D. Užkuraitis. 2022. *Tabletop Exercise: Coherent Resilience Baltic 2021 (CORE 21-B) Final Report*. Joint Research Centre (JRC) Technical Report. https://doi.org/10.2760/74397.

Schaub, Gary, Martin Murphy, and Frank G. Hoffman. 2017. "Hybrid Maritime Warfare: Building Baltic Resilience." *RUSI Journal* 162(1): 32–40. https://doi.org/10.1080/03071847.2017.1301631.

Tessari, Paola, and Karolina Muti. 2021. *Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Wigell, Mikael, Harri Mikkola, and Tapio Juntunen. 2021. *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.