International Journal of Instruction, Technology, and Social Sciences
Vol. 5, 32-38, 2026
ISSN: 2716-6546
www.ijitsc.net

An updated analytical framework on cyber resilience and managing the response to hybrid threats

Daniel Dăneci Pătrău[1,2*], Daniela Simona Nenciu[1], Carmen Elena Coca[1], Oana Bocănete[1], Romeo Boşneagu[1,3], Raluca Ionela Ciortan[1], Anda Cristina Bozgoiu[1]

[1]Tomis University of Constanța

[2]Maritime University of Constanța

[3]Mircea cel Batran Naval Academy of Constanta

*Corresponding author: mail: danusidenima2@yahoo.com

Abstract. The complexity of the international security environment, accentuated by the proliferation of hybrid threats and the increased interdependence between the physical, digital, and social domains, calls for the development of coherent analytical frameworks for managing the response at the national and European levels. Based on recent developments in Romania's eastern neighborhood and in the Euro-Atlantic space—the annexation of Crimea, the protracted conflict in Ukraine, the sabotage of critical maritime infrastructure, and the intensification of cyber and information attacks against democratic states—this article aims to outline a current framework for analyzing hybrid threats and to argue for the central role of cyber resilience and security culture in countering them. The paper is conceptual and exploratory in nature, based on the analysis of strategic and normative documents, specialized literature, and recent case studies. The main result is the proposal of a four-step analytical framework for managing hybrid threats (identifying the adversary's instruments of power, assessing vulnerabilities, identifying likely targets, calibrating the response by strengthening security culture and cyber resilience). The implications of the entry into force of recent European legislation on cybersecurity and digital operational resilience are also discussed..

Keywords: cybersecurity, hybrid threats, cyber resilience, security culture, critical infrastructure.

1. Introduction

The article highlights that cyber resilience is not just a conceptual trend, but a structural element of national security and business continuity, especially in critical sectors. By analyzing recent examples of hybrid warfare (attacks on energy and maritime infrastructure, cyber interference in electoral processes, digitally supported disinformation campaigns), several key lessons are drawn regarding the need to transition from the "it must not happen" paradigm to the "it will happen, but we will continue to function" paradigm.

The events recorded in recent years in the international security environment—the annexation of Crimea, the destabilization of the situation in eastern Ukraine, the large-scale invasion of Ukraine, the proliferation of hostile actions in the cyber and information domains, influence campaigns on electoral processes in Western countries (including the US, France, and Romania) – can be classified as emerging security challenges associated with the phenomenon of hybrid warfare and threats. These developments call for the identification of new approaches to crisis management and the design of an effective framework for cooperation at the national, regional, and Euro-Atlantic levels.

At the European Union and NATO level, the concept of hybrid threats became central to the strategic agenda at the NATO Summit in Warsaw (2016), when combating them was established as a priority area for cooperation. Subsequent strategic documents have emphasized that hybrid activities—disinformation, election interference, cyberattacks, economic and energy pressure, radicalization of vulnerable actors—have become a permanent feature of the European security environment, and the response cannot be merely sectoral or reactive.

At the same time, significant steps have been taken at European Union level to strengthen the cybersecurity framework and the resilience of critical infrastructures: the NIS Directive and subsequently NIS2, the General Data Protection Regulation (GDPR), the PSD2 Directive on payment services, the TIBER-EU framework and, recently, the Digital Operational Resilience Act (DORA) and the Cyber Resilience Act. These developments reflect the recognition that cyberspace has become both a theater of confrontation and a vector for the projection of power.

The interconnection between the physical, digital, and social domains—an effect of the fourth industrial revolution—has reduced the entry costs for state and non-state actors in the use of hybrid means, especially in the cyber and information domains. The hybrid nature of the new types of threats is reflected in the way they manifest themselves below the threshold of open warfare, combining conventional, asymmetric, and unconventional tactics, with cumulative effects in the political, economic, societal, and military spheres.

In this context, the objectives of the article are:

- to clarify the concepts of hybrid threats, national resilience, and security culture;
- to outline a current analytical framework for managing hybrid threats, with an emphasis on the cyber dimension;
- to argue the role of cyber resilience as a central element of the response to hybrid warfare;
- to illustrate, through recent examples and their lessons, how hybrid warfare manifests itself in practice.

2. Materials and methods

The article is predominantly conceptual and exploratory in nature, based on the following types of materials and methodological approaches:

- *Analysis of specialized literature*

Theoretical and applied works on resilience, hybrid threats, and cybersecurity were taken into account: studies devoted to resilience in international relations, works on hybrid warfare and the instruments of power used by state and non-state actors, analyses of security culture and national resilience to hybrid threats, as well as studies on the changing international order and the impact of globalisation and new technologies on security.

- *Analysis of the regulatory and strategic framework*

Strategic and political documents issued at the level of the European Union and NATO were analyzed: the communiqué of the NATO Summit in Warsaw (2016) [10], the joint European Commission-EEAS report on the implementation of the joint framework for countering hybrid threats, the joint EU-NATO declaration [12], as well as relevant regulatory instruments at European level (NIS, NIS2, GDPR, PSD2, TIBER-EU, DORA, the Cybersecurity Resilience Act).

- *Case study and illustrative analysis*

Case studies were used to illustrate the manifestation of hybrid warfare and the vulnerabilities of critical infrastructure, such as: the conflict in Ukraine and the annexation of Crimea; the use of cyber attacks (malware, spear-phishing campaigns) on government systems; the sabotage of the Nord Stream 1 and 2 pipelines in the Baltic Sea (September 2022), as an example of hybrid aggression against critical maritime infrastructure; cyber and information interference in recent electoral processes (US, France, European states, including Romania).

- *Structural analytical approach (four-stage framework)*

Based on the literature and strategic documents, the article proposes a four-stage analytical framework for managing hybrid threats, with a focus on cyber and societal vulnerabilities. The

framework is conceptual, intended to support decision-making and strategic planning, not to provide a quantitative model.

The paper does not attempt a quantitative empirical analysis and does not test hypotheses using statistical methods. It focuses on qualitative analysis and the coherent integration of multiple sources to underpin a framework for analysis and propose courses of action.

3. Results and discussions

For the first time, in July 2016, during the NATO Summit in Warsaw, combating hybrid threats was identified as one of the priority areas for cooperation between the EU and NATO. Following the summit, the joint report by the European Commission and the European External Action Service described the European security environment as being significantly affected by hybrid actions: "Hybrid activities are becoming a frequent feature of the European security environment. The intensity of these activities is increasing, with growing concerns about election interference, disinformation campaigns, hostile cyber activities, and hybrid actors seeking to radicalize vulnerable members of society to act on their behalf" [11].

In this way, it is recognized, in practice, not only that the impact of hybrid threats exceeds the territory of Member States, being felt at European level, but also that "European security has become a negotiated, contested, and contested issue" [7], as a result of new challenges arising from the actions of state and non-state actors. Recognizing the complex and cross-border nature of hybrid threats, this framework has proposed to EU member states an administration-wide approach to strengthen the overall resilience of our societies.

Hybrid threats refer to the methods and instruments used by a potential aggressor - state or non-state - to support its own interests, strategies, and objectives in relation to an adversary, by combining military and non-military, conventional and unconventional means, in an integrated manner and often below the threshold of classic armed conflict. They are characterised by:

- multidimensionality - simultaneous actions in the military, political, economic, informational, cybernetic and energy spheres;
- ambiguity and deniability - the difficulty of clearly identifying the aggressor and distinguishing between peace and war; exploitation of internal vulnerabilities – economic, social, political, regulatory, cultural;
- difficulty of verification and attribution - the links between activities are unclear, fragmented, and difficult to prove.

While hybrid warfare involves the escalation and synchronization of instruments of power in an open conflict setting, hybrid threats describe a pre-conflict reality characterized by hostile actions below the threshold of declared use of armed force, but which may prepare the ground for escalation.

Based on recent literature and developments, several major factors contributing to the emergence and intensification of hybrid threats can be identified:

- the changing post-Cold War international order, globalization and advanced communications technologies, the emergence of new areas of confrontation, particularly cyberspace;
- the exploitation of new media technologies and social networks for influence;
- the blurring of the boundary between peace and war through the predominant use of unconventional means.

The proposed four-stage framework includes:

- identifying the adversary's instruments of power - propaganda, media control, social media, fake news, information leaks, cyberattacks, etc.;
- assessing internal vulnerabilities - critical functions, digital dependencies, geographical, social, political, and economic vulnerabilities;
- identifying the adversary's objectives - undermining trust, influencing strategic orientation, gaining economic and energy advantages;

- calibrating the response – through public policies, legal instruments, strengthening the security culture, and developing cyber resilience.

Cyber resilience is defined as an entity's ability to continuously deliver the desired outcome despite adverse cyber conditions and involves: changing the managerial mindset (accepting the inevitability of successful attacks); shifting from an exclusive focus on prevention to limiting consequences; early detection and limiting the spread of incidents; redundant and flexible IT architectures; integration of technical, organizational, and human measures.

Analysis of recent patterns of hybrid actions indicates the following trends specific to the forms of manifestation of threats identified predominantly in the information and cyber domains and which can be found in the integrated strategies of a potential aggressor in an aggression scenario:

- *The use of propaganda as a prevalent means of action*

We are currently witnessing "the militarization and transformation of information into a weapon of war," as stated in the communiqué of the NATO Summit in Warsaw in July 2016. What is new is the means used in propaganda actions. New media technologies and social networks can be vectors of information aggression. They are used to maximize the effects of a campaign in a hybrid confrontation.

- *Control over subservient domestic media sources with a wide audience, both inside and outside the aggressor state.*

Subservient media outlets become very influential when the material they publish is picked up by popular foreign media sources, as was evident from the Joint Declaration adopted at the NATO Summit in Warsaw on July 7-8, 2016.

- *Social media does indeed offer new opportunities for a potential aggressor seeking to gain access to the media and the general public of the targeted countries*.

Disinformation campaigns can be particularly effective given the high prevalence of news consumption via social media among the general public.

- *The widespread use of fake news to influence the perception of target audiences.*

Fake news is more than just false news. It includes information that deliberately distorts the objective truth for the consuming public and pursues a specific goal, usually associated with satisfying the hostile interests of a potential aggressor. Unlike fake news, false news is or may be generated by causes that denote superficiality in journalistic documentation or lack of professionalism, but also by interests derived from editorial policy that may be reflected in the biased or less objective presentation of informational content.

- *The existence of platforms that facilitate the publication of data classified as information leaks, obtained through cyber espionage (actions of this kind are said to have been carried out in recent elections in the US and Romania).*

In December 2024, the Cybersecurity Act came into force to make Europe's cyberspace safer and more secure. This marks a major leap forward in the EU's efforts to protect its citizens and businesses from cyber threats.

The Cybersecurity Resilience Act (CRA) is the first EU legislation to introduce mandatory cybersecurity requirements for products that include digital elements.

The law introduces greater responsibilities for manufacturers to ensure the security of hardware and software products. At the heart of the law are new obligations for manufacturers to provide software updates that address security vulnerabilities and provide security support to consumers. By increasing transparency on cyber risks and product security, the law enables consumers to make informed choices about products available on the EU market. Products will bear the CE marking to indicate that they comply with the requirements of the regulation. The main obligations of the law will apply from December 11, 2027.

Henna Virkkunen, Executive Vice-President of the European Commission, said: "We are committed to making Europe a safe and secure place for our citizens and businesses to operate. This new regulation is an important step forward in ensuring that digital products in the EU do not pose cyber risks to EU consumers."

The Cybersecurity Act complements the NIS2 cybersecurity framework, which entered into force on January 16, 2023, and was implemented in national legislation by October 17, 2024. It is part of a comprehensive set of measures that the EU is putting in place to strengthen the cybersecurity of an increasingly digital and connected Europe.

Companies in regulated economic areas have long been forced to invest in IT security, and for a long time the approach has been: "to protect ourselves, we take the best solution for this risk or attack vector." The concept of "defense in depth" emerged, areas of overlap between solutions began to appear, and tools based on machine learning and artificial intelligence appeared. Meanwhile, the complexity of auditing and compliance has also increased, resulting in many more controls.

Cyber resilience encompasses all of these and focuses on risk mitigation, but from a different perspective. In practice, cyber resilience is the ability of an entity to continuously deliver the desired result despite adverse cyber conditions. From this point of view, the authors believe that the first thing an organization needs to develop cyber resilience is a change in mindset, i.e., top managers need to understand that there will be successful attacks. The offensive area has become so complex that it is practically guaranteed that at least one service within the company will be compromised at some point.

Next, we recommend shifting the focus to how the consequences can be mitigated, so that defense against cyber attacks can begin as early as possible, after the first signs of compromise, and the tools used by the company can prevent the next steps of the attack from being carried out, in order to continue operations in good security conditions.

Relevant examples of hybrid warfare include: Russia's involvement in Ukraine, through a combination of energy pressure, support for separatists, cyber attacks, and disinformation campaigns, culminating in the illegal occupation of Crimea (2014); China's use of hybrid instruments in the South China Sea; Iran's development of offensive cyber capabilities, coupled with internal control of energy resources and the media; the modus operandi of non-state actors (Hezbollah, Al-Qaeda, Islamic State), which combine terrorist, informational, and political tactics.

To highlight the practical relevance of the proposed framework, several recent examples are presented, together with the main lessons learned:

- ***Sabotage of the Nord Stream 1 and 2 pipelines (Baltic Sea, 2022)***

The sabotage of the Nord Stream 1 and 2 pipelines in the Baltic Sea (September 2022) is a prime example of hybrid aggression against critical maritime energy infrastructure. The attack took place outside a formal framework of declared conflict, the responsible actor was not unanimously identified, and the consequences went beyond the bilateral level, affecting European energy security.

Lessons learned: underwater infrastructure (pipelines, communication cables) is a strategic target in hybrid warfare; the lack of clear attribution creates strategic ambiguity and reduces classic response options; There is a need to develop joint EU-NATO mechanisms for monitoring, protection, and response in the field of submarine infrastructure; resilience is not only about technical remediation, but also about managing the economic and political impact.

- ***Cyberattacks on the Ukrainian energy network (2022–2023)***

In the context of the conflict in Ukraine, cyber attacks on energy networks and critical infrastructure perfectly illustrated the integration of the digital dimension into military and hybrid strategy. Groups associated with Russian intelligence services used advanced malware to disrupt industrial control systems and cause power outages.

Lessons learned: cyber attacks can be used to amplify the effects of traditional military campaigns, increasing pressure on the population; protecting ICS/SCADA systems is becoming a priority for all states with critical energy infrastructure; international cooperation in the exchange of information and technical assistance (e.g., support from NATO, the EU, partners) is essential; continuity plans must explicitly include scenarios of cyber attacks coordinated with military actions.

- ***Disinformation and deepfake campaigns in recent elections***

In recent years, multiple countries have reported coordinated disinformation campaigns in the context of elections, based on fake news, algorithmic manipulation of content, and, increasingly, the use of audio-video deepfakes to discredit candidates or amplify social polarization.

Lessons learned: the cognitive and informational space is the center of gravity of many modern hybrid operations; developing societal resilience requires media literacy, critical thinking, and credible fact-checking mechanisms; electoral authorities and media institutions must collaborate to implement rapid procedures for identifying and countering manipulative content; a culture of security is needed to enable early recognition of hostile narratives and refuse their political exploitation.

Common lessons for the analytical framework

Several cross-cutting lessons can be drawn from these examples: the need for an integrated vision: no incident should be viewed strictly as a "cyberattack" or "energy incident," but rather as part of a broader hybrid scenario; The primacy of response time: early detection and rapid response are crucial to limiting the cumulative effect of hybrid actions. The centrality of resilience: states and organizations must start from the premise that aggression cannot be completely prevented, but its impact can be managed, limited, and absorbed. The role of security culture: informed populations and prepared institutions are less vulnerable to panic, manipulation, and demoralization during a hybrid attack.

4. Conclusions

The intensification of hybrid threats and forms of hybrid warfare requires the development of integrated risk and crisis management approaches, in which cyber resilience and security culture play a central role.

The main conclusions are:

- Hybrid threats are structurally multidimensional and difficult to attribute, designed to exploit internal vulnerabilities and manifest themselves below the threshold of armed conflict. They combine military and non-military, digital and physical instruments, with cumulative effects on national security.
- The proposed four - step analytical framework – identifying instruments of power, assessing vulnerabilities, identifying adversary objectives, calibrating the response through security culture and cyber resilience—provides a useful conceptual tool for policymakers and security practitioners.
- Cyber resilience is not just an innovative concept, but a strategic necessity, especially for critical infrastructure operators and organizations that depend on digital services. Accepting the inevitability of successful attacks and shifting the focus from absolute prevention to limiting consequences and ensuring business continuity are essential.
- Security culture and the human component are just as important as technical measures. Without a change in mindset—from "it must not happen" to "it will happen, but we are prepared"—public bodies and private organizations risk reacting too late and ineffectively.
- Recent examples of sabotage of energy and maritime infrastructure, cyberattacks on energy networks, and disinformation campaigns in electoral contexts show that cyberspace and the cognitive domain are increasingly becoming primary fields of confrontation. The lessons learned from these cases must be systematically integrated into public policy, military planning, and corporate governance.

Future research directions include the development of quantitative indicators of cyber resilience, empirical analysis of the impact of security culture measures, and modeling of response scenarios to hybrid attacks on critical infrastructure.

References

[1] R. BACH, D. KAUFMAN, K. SETTLE, M. DUCKWORTH, Policy Leadership Challenges in Supporting Community Resilience. Strategies for Supporting Community Resilience. Crisis Management Research and Training: Multinational Experiences, Swedish Defence University, Stockholm. The paper is available at http://fhs.diva-portal.org/smash/get/diva2:795117/FULLTEXT01.pdf, (2022).

[2] A. BUSLA, Combined Method of Sight Reduction. TransNav – The International Journal on Marine Navigation and Safety of Sea Transportation, 15(2), 389–393. DOI: 10.12716/1001.15.02.16, (2021).

[3] P. BORBEAU, Resilience and International Politics: Premises, Debates, Agenda. International Studies Review. Available at: https://doi.org/10.1111/misr.12226, (2015).

[4] P.J. CULLEN, E. REICHBORN-KJENNERUD, Understanding Hybrid Warfare. London: Multinational Capability Development Campaign (MCDC) 2016–17, (2023).
[5] T. FRUNZETI, C. BĂRBULESCU, National resilience to hybrid threats and security culture. Available at: https://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf, (2018).
[6] D. HAMILTON, Forward Resilience. Protecting Society in an Interconnected World. Center for Transatlantic Relations, (2022).
[7] S. MATTI, Hybrid threats – what are we talking about? European Center of Excellence for Countering Hybrid Threats, Helsinki. Available at: https://www.hybridcoe.fi/news/hybrid-threats-what-are-we-talking-about/, (2017).
[8] K. ROER, Build a Security Culture. IT Governance Publishing, (2021).
[9] H. VAN SOEST, J. BLACK, H. FINE, L. RETTER, Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience. RAND Europe. Available at https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3800/PEA3800-1/RAND_PEA3800-1.pdf, (2025).
[10] NATO, Communiqué of the NATO Summit in Warsaw, July 2016. Available at: https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummit Communique.pdf, (2016).
[11] EUROPEAN COMMISSION & EUROPEAN EXTERNAL ACTION SERVICE, Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – A European Union response, p. 3. Available at: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017JC0030&from=RO, (2017).
[12] NATO & UE, Joint Declaration adopted at the NATO Summit in Warsaw, July 7–8, 2016, (2016).