DEFENCE THROUGH STRATEGIC ACTIONS AGAINST POTENTIAL HYBRID THREATS

Assoc. Prof. Mariana Rodica ŢÎRLEA, PhD

"Dimitrie Cantemir" Christian University, Bucharest

ORCID: https://orcid.org/0000-0002-0665-5839

JEL: K30, K33

DOI: 10.55535/RMT.2026.1-2.08

The world of exponential change is marked by multiple risks that loom everywhere. Peace requires social, economic, and educational protection, strategic resilience, and security in border defence, combined with partnerships and collaborations. In this context, shaped by the evolving security environment both globally and regionally, there is an urgent need to identify potential threats and conduct impact studies based on scenario-building methods, forecasts, and planning for potential civil intervention and emergency actions. The resulting solutions should, on the one hand, be managed and disseminated in a timely manner and, on the other hand, support decision-making processes at the military, political, and administrative levels.

The unpredictable nature of current developments, the transformations ocurring in the regional and international environment, and the pace of change require the continuous review of the scenario-based findings and conclusions. This review must be carried out in an active, proactive, and creative manner with regard to the projected, identified solutions, applied methods and models, including the development of new scenarios. All these factors generate continuous change that requires rapid adaptability, continuous involvement from working groups, the use of AI for effective management and governance, and the implementation of optimal measures and decisions to counter hybrid threats.

Keywords: hybrid threats; impact studies; scenario method; planning; strategic resilience;

INTRODUCTION

The current reality indicates a significant increase in security risks generated by phenomena such as armed conflicts and hybrid wars/threats, which require a multidimensional and coordinated approach both in the management of crisis situations and in the development of national and international security strategies. In the 21st century, under the impetus of multivalent technological progress, globalisation has reduced distances, significantly influencing the international security environment: *"Generated by the unprecedented development of technologies, especially in the fields of transport and communications, globalisation has led to the emergence of processes of time-space compression and the diminishing relevance of national borders, which considerably influence the evolution of the international security environment. Although states remain the main actors of the international system, a range of non-social actors have emerged alongside them, becoming voices on the international arena, voices at least as influential as those of state actors"* (Frunzeti, 2020, p. 9).

In the 21st century, under the impetus of multivalent technological progress, globalisation has reduced distances, significantly influencing the international security environment.

Referring to the concept of *hybrid warfare*, the specialised literature uses a variety of terms, including: *hybrid threats, hybrid influence* or *hybrid adversary* (as well as concepts such as *nonlinear warfare, non-traditional warfare* or *special warfare*) to describe a wide range of conflict manifestations. American military institutions often use the term *hybrid threats*, while academic literature prefers the phrase *hybrid warfare* (Simileanu, 2018, pp. 33), conceptualised as a *"multimodal asymmetric conflict"* (Ibid., p. 34). For the purpose of conceptual clarification, *table 1* presents the most relevant definitions identified in specialised sources consulted in order to elaborate this material.

Table 1: Conceptual framework of hybrid threats[1]

No.	Concept	Explanation
1.	**To threaten**	1. To express an intention to cause harm to someone (to intimidate them or to obtain something from them). 2. To make a threatening gesture. 3. To pose a danger to someone or something.
2.	**Threat**	1. The act of *threatening* and its result. 2. The expression, through words, gestures, etc., of an intention to cause harm or inconvenience. 3. A danger or peril. 4. A criminal offense that consists of alarming a person by expressing the intention to commit a crime or harmful act against them or a close relative.
3.	**Threat**	(Long-term) armed conflicts between two or more states, nations, groups for pursuing economic and political interests.
4.	**Hybrid threats**	1. *"The combination of conventional and unconventional, military and non-military, overt and covert actions, the aim of creating ambiguity and confusion on the nature, the origin and the objective of the threat; the ability to identify and exploit vulnerabilities of the target; the ability to keep the level of hostility below the threshold of open conventional warfare"* (Anderson, Tardy, 2015). 2. Hybrid threats are coordinated harmful activities, carried out with malicious intent, aimed at undermining a target, such as a state or an institution[2].

[1] According to https://dexonline.ro/definitie/amenin%C8%9Bare.
[2] https://www.bing.com/search?pglt=43&q=Amenin%C8%9B%C4%83ri+hibride&cvid=c95f2ac10cdc4ff4ab97cb0.

No.	Concept	Explanation
5.	**War**	A short or long-term conflict between two or more groups, social categories or states pursuing financial, ethnic, territorial, economic and/or political interests (dexonline.ro).
6.	**Civil war**	Armed struggle waged for the purpose of seizing power or achieving political supremacy within a state (dexonline.ro).
7.	**Information warfare**	Actions intended to achieve information superiority by compromising an enemy's information systems while protecting one's own information resources. According to the US Department of Defense: *"actions taken to achieve information superiority in support of national military strategy by affecting enemy information and information systems while leveraging and defending friendly information and information systems".* (Solescu, 2000)
8.	**Hybrid warfare**	It is a combination of conventional and unconventional tactics, including cyberattacks, disinformation campaigns and economic pressure, used to undermine a state's stability without resorting to direct armed conflict.
9.	**World war**	An armed conflict involving directly or indirectly numerous states around the world (dexonline.ro).
10.	**Cold war**	A state of tension in relations between states, particularly between the United States and the Soviet Union after 1950 (dexonline.ro).
11.	**Psychological warfare**	A state of tension and psychological pressure deliberately created and maintained to undermine the morale of opposing forces and demoralise the population (dexonline.ro).

No.	Concept	Explanation
12.	**Total war**	An armed conflict in which the aggressor state uses all available means of destruction not only against military forces but also against the civilian population (dexonline.ro).
13.	**Full-spectrum warfare**	Encompasses a wide range of integrated military and non-military instruments of state power and clandestine actions available to a hybrid actor. (Chifu, Grigore, 2025, p. 15).
14.	**Strategic superiority**	Achieved through *"the development of Autonomous Weapon Systems (AWS) or even Lethal Autonomous Weapon Systems (LAWS) as a major advantage"* (Barac, 2025, p. 183; Stancu, 2025, p. 183).

Therefore it can be observed that *"there are periods in the history of mankind during which political, social or economic events generate changes, transformations and even innovations in the field of thought and reflection, across all its dimensions. The military dimension of such periods could not escape efforts to generate new concepts and ideas, many of which eventually evolved into substantial and enduring doctrines"* (Papoi, 2017, p. 130).

MANIFESTATIONS OF VIOLENCE WITHIN THE FRAMEWORK OF HYBRID OPERATIONS

Hybrid threats manifest themselves through a variety of forms of violence and complex actions, characterised by:

- initiatives of the adversary with the intention of influencing and destabilising the domestic environment;
- the use of advanced technologies, including artificial intelligence, facial recognition technologies and intelligence-gathering methods, aimed at collecting information;
- the exploitation of critical targets, such as critical infrastructure and energy and industrial resources, with the aim of disrupting the normal functioning of society;

- specialised communication and disinformation campaigns designed to generate confusion and chaos;
- asymmetric and non-linear methods of warfare, as well as actions aimed at domination, control, and the attainment of supremacy;
- extended preparation periods and response strategies adapted to different phases of a conflict;
- the use of terrorism and subversion for destabilisation and intimidation;
- the maintenance of a climate of instability, fragmentation frozen conflicts, and political diversion.

"The current geostrategic context and the security climate in which we find ourselves require rapid adaptation to ongoing changes, regardless of whether these relate to economic, social, political or, especially, security-related issues" (Bălan, 2025, p. 9).

"In this complex landscape, Romania no longer has the luxury of neutrality" (Barac, p. 9).

In the face of hybrid threats, the European Union faces a series of complex challenges, that complicate efforts to identify, prevent and counter such risks. In particular, we can highlight three key elements that significantly influence the EU's ability to respond effectively:

In the face of hybrid threats, the European Union faces a series of complex challenges, that complicate efforts to identify, prevent and counter such risks. In particular, we can highlight three key elements that significantly influence the EU's ability to respond effectively: differences among member states; heterogeneity; limitations of the legislative harmonisation.

1. *Differences among member states:* one of the most important obstacles to the coordination and implementation of common measures against hybrid threats is the diversity of interests, levels of development, capabilities and priorities among member states. This heterogeneity results in varying perceptions of risk, different levels of resource allocation and distinct approaches to security issues. Thus, coordinating a common response becomes difficult, while interoperability between national and European structures may be affected, reducing the efficiency of the entire collective security and defence system.

2. Heterogeneity: economic, legal, institutional, cultural, natural resource and environmental dimensions. The European Union comprises states with different socio-economic and cultural contexts, as well as with distinct institutional structures. This diversity leads to variations in legislative framework, administrative capacities and the preparedness of security and defence structures. For example,

differences in legal regulations and in the capacity to implement policies may create gaps within the common defence system. In addition, disparities in natural resources and environmental conditions may shape specific vulnerabilities to hybrid attacks, such as those targeting critical infrastructure, energy systems or cyberspace.

3. Limitations of the legislative harmonisation: another critical issue concerns the opportunities and limitations associated with harmonising national legislation with European directives and regulations. Although a common European framework exists for addressing hybrid threats, implementation at the national level varies according to each country's specific circumstances. As a results, a minimum common standard is achieved which, while necessary, is not always sufficient to ensure coherent and effective protection of citizens' interests and critical infrastructures.

EU member states transpose and implement European directives according to their own national circumstances, taking into account their specific resources and requirements, which may result in variations in the application of European rules.

In conclusion, these three factors represent major obstacles to building an effective common defence against hybrid threats. Overcoming these challenges requires intensified cooperation and coordination, as well as the development of flexible instruments and mechanisms, adapted to the national specificities while ensuring the coherence and unity of the European response.

The EU acquis on hybrid threats includes the NIS 2 Directive on cybersecurity and the CER Directive on the resilience of critical entities – which replaces Directive 2008/114/EC. In this regard, adherence to and alignment with the European acquis on cybersecurity and hybrid threats constitute fundamental pillars for ensuring effective and coordinated defence at regional and international level.

EU member states transpose and implement European directives according to their own national circumstances, taking into account their specific resources and requirements, which may result in variations in the application of European rules. Countries neighbouring the EU adopt the Union's security models and integrate them into their national systems, while candidate countries implement the aquis communautaire to align themselves with European standards. By applying these frameworks, the aim is to establish a minimum level of harmonisation, ensuring a common basis for security and protection throughout the Union. In this context, we can recall the European Parliament Report of 28 February 2024, which focuses on strengthening

EU support for Ukraine, enhancing partnership with like-minded partners and allies to ensure the successful implementation of the CSDP (Common Security and Defence Policy), reinforcing EU security and defence capabilities, complementing security and defence policies with civilian instruments and strengthening complementarity with NATO while preserving European strategic autonomy. The report also sets the ambition of transforming the EU into a strategic international security provider through deeper integration in the field of defence (https://www.europarl.europa.eu/factsheets/ro/sheet/159/politica-de-securitate-si-aparare-comuna).

A POSSIBLE STRATEGIC MODEL FOR IDENTIFYING HYBRID THREATS

According to the conceptual model we propose, the process of identifying and managing hybrid threats should follow several stages, ranging from preliminary analysis to consequence assessment and the restoration of normality. This model aims, in our opinion, to support the creation of a stable and favourable environment in which knowledge, predictability and resilience are ensured, as well as to minimise the impact of hybrid threats on national and regional security *(table 2).*

Table 2: Strategic model for identifying hybrid threats (author's conception)

No.	Stages	Activities to be carried out
1.	Identification of potential crisis-related threats	Studies to identify potential crisis threats in the following areas: economic; legal; institutional; cultural; natural resources; environmental resources. Selection of potential crisis situations. Analysis of selected crisis situations. Obtaining results. Verification of results in order to build a list of possible crisis situations.

No.	Stages	Activities to be carried out
2.	Development of a list of potential crisis situations	Based on the results of Stage I, a list of potential crisis situations will be drawn up.
3.	Risk analysis for selected potential crisis situations	Identification of threats in the following areas: economic; legal; institutional; cultural; natural resources; environmental resources. Activities include: – risk estimation; – risk assessment; – estimation of potential effects; – development of response solutions to threats associated with selected crisis situations.
4.	Development of a crisis program	Preparation of a crisis programme based on the identified list of potential crisis situations.
5.	Threat-level risk management	Designation of a team with clearly defined responsabilities.
6.	Early identification of crisis situations	Actions supported by artificial intelligence.
7.	Simulations for anticipated crisis-response situations	Actions supported by artificial intelligence.
8.	Anticipated response actions for crisis situations	Actions supported by artificial intelligence.
9.	Assessment of the consequences of the crisis situation	Evaluation of all types of demages.
10.	Restoring the initial state	Achieving the pre-crisis state.
11.	Analysis of the crisis	Conducting post-crisis analyses.
12.	Identification of the causes of the crisis	Determining the actual causes that generated the crisis.

No.	Stages	Activities to be carried out
13.	Special post-crisis programmes	Developing scenarios for newly emerged situations and correlating them with historical data and information.
14.	Special programs for unforeseen situations	Building scenarios for unforeseen situations.
15.	Decision-making process programme	Development of specific decision-support tools adapted and implemented in real time.

Such a strategic model for identifying hybrid threats, based on clearly defined stages and specific procedures for analysis, assessment and response, could, in our opinion, serve both a planning and control tool and could contribute to strengthening response capabilities at national and international levels. This model would facilitate a proactive and adaptive approach, which would enable an effective management of emerging risks. As such, we believe that the implementation of such a strategic framework would generate several benefits, such as:

Through the early identification of hybrid threats, protection and resilience measures can be implemented for critical infrastructures, IT systems and communication networks.

❖ Supporting a stable IT, logistical, technological environment – through the early identification of hybrid threats, protection and resilience measures can be implemented for critical infrastructures, IT systems and communication networks. This reduces the vulnerability of essential systems and ensured the continuity of economic, administrative and military activities. In addition, strengthening technological and logistical infrastructure becomes an integral part of the prevention strategy.

❖ Developing knowledge and strategic vision – assessing and monitoring hybrid threats stimulates the accumulation of relevant information, creating a knowledge base for the development and constant adjustment of security policies. In addition, this approach facilitates the formation of an integrated understanding of the security environment, supporting informed and coherent decision-making.

❖ Strengthening and raising awareness of education – implementing a systematic model for identifying and managing hybrid threats also requires continuous education and training of personnel

involved in the security field, as well as among the population. Raising awareness contributes to the development of a resilient society capable of recognising and responding effectively to hybrid events.

❖ Promoting institutional unity and coherence – a coordinated and common process for identifying and responding to hybrid threats ensures effective collaboration among different defence, intelligence, security and crisis management institutions and structures. This institutional unity is fundamental to avoid duplication of efforts and to create a common front against adversaries.

❖ Enhancing national and regional security – by monitoring and anticipating hybrid threats, preventive measures can be implemented to reduce the risk of conflict escalation and destabilising events. Thus, a higher level of general security is ensured for both citizens and strategic infrastructures.

A well-defined strategic model enables the early identification of vulnerabilities and weak points, facilitating the adoption of prevention and mitigation measures. This contributes to preventing large-scale hybrid attacks, as well as reducing the impact of adverse events on society.

❖ Avoiding and reducing vulnerabilities – a well-defined strategic model enables the early identification of vulnerabilities and weak points, facilitating the adoption of prevention and mitigation measures. This contributes to preventing large-scale hybrid attacks, as well as reducing the impact of adverse events on society.

❖ Minimising the consequences of adverse events – by applying an adapted prevention and response system, the harmful effects of hybrid attacks can be limited, reducing human, economic and social costs. In addition, this process supports rapid and efficient recovery after incidents, ensuring the stability and continuity of the functioning of critical systems.

"The future is not written in binary code, but in choices. And choices, especially in the field of security, must be made lucidly, responsibly and – above all – consciously" (Barac, 2025, p. 9).

"The increase in risks and threats in the geopolitical and strategic security environment, as well as in cyberspace, creates conditions for increasing the vulnerabilities of military communication and information systems for command and control. There is a need for effective and timely implementation of protection measures for own systems, as well as for the development of cyber defence capabilities compatible with those of NATO member states" (Prokopiev, Pavlova, Vasileva, 2025, p. 319).

In conclusion, adopting such a strategic model for identifying and managing hybrid threats represents a fundamental approach to strengthening national and regional resilience. It facilitates integrated, proactive and adaptive risk management, contributing to the creation of a safer, more stable and future-ready environment based on the *"early identification of radicalisation patterns"* (Dragomir, 2025, p. 168), particularly in a context where *technology will play an increasingly important, and in some cases critical, role* (Ibid., p. 226).

CONCLUSIONS

Hybrid threats represent a complex phenomenon, characterised by diverse and often subversive manifestations that exist in the grey zone between peace and war. Addressing and countering these risks require a continuous culture of knowledge and education, as well as the implementation of proactive measures of anticipation and resilience. In addition, it is essential to develop integrated strategies that include:

- the capacity to anticipate and adapt to rapid changes in the global environment, in which sense we have developed a model for identifying hybrid threats, presented in 11 gradual stages designed to support the identification of potential hybrid threats;
- resilience in the face of disasters, understood as the capacity to withstand and respond to adverse events – whether deliberate, accidental or natural – and to return as quickly as possible to a minimum functional level.

Hybrid threats represent a complex phenomenon, characterised by diverse and often subversive manifestations that exist in the grey zone between peace and war. Addressing and countering these risks require a continuous culture of knowledge and education, as well as the implementation of proactive measures of anticipation and resilience.

The transition of society towards the digital age and artificial intelligence represent major challenges, requiring an adapted legislative framework and an ethical approach to ensure that technological benefits are harnessed responsibly. Anticipating future risks and opportunities has become a crucial component of security and development strategies, enabling societies to adapt proactively to the rapid transformations of the global environment.

Clarity in security rules and procedures is an essential pillar for ensuring a common understanding and the effective implementation of protective measures. A minimum framework for the protection of critical infrastructure is required to prevent vulnerabilities and ensure the continuity of societal functioning. The required level of protection

should be adapted to the realities of each country while maintaining a common standard capable of guaranteeing security. Last but not least, a minimum system for emergency preparedness and response is essential for effectively addressing threats and protecting both the population and critical infrastructure.

BIBLIOGRAPHICAL REFERENCES:

1. Anderson, J.J., Tardy, Th. (2015). *Hybrid: What's In a Name? European Union Institute for Security Studies*, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_32_Hybrid_warfare.pdf, retrieved on 10 November 2025.
2. Barac, M. (2025). *Gândind securitatea dincolo de tipare – între algoritmi, doctrine şi frontiere fragile*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. Bucureşti: Statul Major al Apărării, nr. 2/2025, https://gmr.mapn.ro/pages/gmr-2-2025, retrieved on 21 February 2026.
3. Bălan, C.D. (2025). *Vulnerabilitatea României în fața amenințărilor hibride din spectrul dezinformării. Imperativul creării unei strategii naționale de combatere a fake news și a structurii necesare implementării acesteia*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. Bucureşti: Defence Staff, nr. 1, https://gmr.mapn.ro/pages/gmr-1-2025, retrieved on 21 February 2026.
4. Chifu, I. (2025). *Construirea unui studiu prospectiv pentru lumea de mâine*, in *GMR Proceedings – 2025*, DOI: 10.55535/, GMR.2025.3.13, https://gmr.mapn.ro/pages/lucrarile-conferintei-2025, retrieved on 22 February 2026.
5. Chifu, I., Grigore, C. (2025). *Război cu spectru larg – de la extinderea instrumentelor la a gândi inimaginabil*, in *Gândirea militară românească* Journal, DOI: 10.55535/GMR.2025.2. Bucureşti: Defence Staff, nr. 2, https://gmr.mapn.ro/pages/gmr-2-2025, retrieved on 21 February 2026.
6. Dragomir, F.L. (2025). *Arhitectură multilevel a sistemelor informaționale pentru monitorizarea tendințelor de radicalizare în mediile digitale*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. Bucureşti: Defence Staff, nr. 2, https://gmr.mapn.ro/pages/ gmr-2-2025, retrieved on 21 February 2026.
7. Frunzeti, T. (2010). *Complementaritatea viziunilor de securitate ale NATO şi UE*, în *Revista de studii politice, relații internaționale și studii de securitate*, vol. I, Sibiu: Editura Universității "Lucian Blaga".
8. Papoi, A. (2017). *Arta militară universală şi națională – idealism şi pragmatism în publicațiile Statului Major General*, in *Gândirea militară românească* Journal. Bucureşti: Defence Staff, nr. 2, https://gmr.mapn.ro/pages/arhiva-revistei, retrieved on 22 January 2026.

9. Prokopiev, S., Aleksandrova, V. Pavlova, E., Vasileva, V. (2025). *Utilizarea poligoanelor cibernetice pentru instruirea în domeniul securității cibernetice ca plan de acțiune în fața amenințărilor hibride*, in *GMR Proceedings – 2025*, DOI: 10.55535/GMR.2025.3, https://gmr.mapn.ro/pages/lucrarile-conferintei-2025, retrieved on 22 February 2026.
10. Simileanu, V. (2018). *Războiul hibrid: abordare conceptuală*, în *Revistă ştiinţifico-practică*, nr. 1/2018.
11. Stancu, A.R. (2025). *Sisteme de luptă autonome – provocări de natură etică*, in *Gândirea militară românească* Journal, DOI: 10.55535/GMR.2025.2. Bucureşti: Defence Staff, nr. 2, https://gmr. mapn.ro/pages/gmr-2-2025, retrieved on 21 February 2026.
12. Solescu, M. (2000). *Impactul războiului informațional asupra societății contemporane*, în *Buletin științific*, nr. 2, Sibiu: Academia Forțelor Terestre.
13. https://dexonline.ro/definitie/amenin%C8%9Bare, retrieved on 22 November 2025.
14. https://www.bing.com/search?pglt=43&q=Amenin%C8%9B%C4%83ri+hibride&cvid=c95f2ac10cdc4ff4ab97cb0, retrieved on 10 November 2025.
15. https://www.europarl.europa.eu/factsheets/ro/sheet/159/politica-de-securitate-si-aparare-comuna, retrieved on 4 November 2025.