Životić, I., & Obradović, D. (2026). EU and NATO responses to hybrid threats: Operational gaps and strategic misalignment, *SCIENCE International journal, 5*(2), 191-195. doi: 10.35120/sciencej0502191z UDK: xxx

EU AND NATO RESPONSES TO HYBRID THREATS: OPERATIONAL GAPS AND STRATEGIC MISALIGNMENT

Ilija Životić[1*], Darko Obradović[2]

[1]Beopolis University, Serbia , e-mail: ilija.zivotic@beopolis.edu.rs
[2]Center for Strategic Analysis, Serbia , e-mail: darkoobradovitch@gmail.com

Abstract: This paper conducts a conceptual policy analysis of hybrid threats and the responses developed by the European Union (EU) and the North Atlantic Treaty Organization (NATO) since 2016. Hybrid threats are understood as coordinated and synchronized actions that deliberately target systemic vulnerabilities of democratic states and institutions, operating across multiple domains while exploiting the thresholds of detection and attribution (Hybrid CoE, 2024). In this context, Foreign Information Manipulation and Interference (FIMI) is examined as a central instrument of contemporary hybrid activity, defined as a coordinated pattern of behavior aimed at undermining political processes and democratic values (EEAS, 2025).

The paper addresses two research questions: how the EU and NATO operationalize counter-hybrid efforts, and what structural gaps persist in their approaches. The analysis focuses on key institutional mechanisms, including the EU's Hybrid Fusion Cell, FIMI analytical framework, and Hybrid Toolbox, as well as NATO's counter-hybrid support teams and the ABCDE methodology.

The findings indicate that both organizations have made significant progress in developing situational awareness and resilience-building capacities. However, their responses remain unevenly operationalized. While NATO demonstrates a higher degree of operational integration, particularly in intelligence and rapid response, the EU's approach is primarily regulatory and coordination-driven.

The analysis identifies two persistent challenges. First, the problem of attribution continues to limit the effectiveness of both political and strategic responses, as hybrid operations are designed to obscure responsibility. Second, insufficient coordination between the EU and NATO reduces the overall coherence of the Euro-Atlantic response framework.

The paper argues that the commonly described complementarity between the EU and NATO remains only partially realized in practice. It concludes by proposing the development of a joint EU–NATO attribution protocol and shared analytical standards, particularly in the use of exposure matrices, as necessary steps toward more effective and synchronized responses to hybrid threats.

Keywords: hybrid threats, disinformation, EU, NATO, cyber security
Field: Social Sciences and Humanities

1. INTRODUCTION

Hybrid threats should not be understood as a new category of security challenges, but rather as a transformation in how power is exercised in contemporary international relations. What distinguishes them is not simply the combination of military and non-military instruments, but the deliberate targeting of systemic vulnerabilities within democratic societies. These vulnerabilities include political polarization, dependence on digital infrastructure, and openness of information environments, which together create conditions in which external actors can influence decision-making without direct confrontation. Hybrid threats can also be understood as a continuation of complex warfare dynamics involving both conventional and non-conventional actors (Mansoor & Murray, 2012; Bajarunas, 2020)

In this sense, hybrid threats operate less as instruments of war and more as tools of strategic influence. Their objective is not immediate territorial control, but long-term shaping of political outcomes. This is particularly visible in the increasing use of disinformation campaigns, cyber operations, and economic pressure as mechanisms for altering public perception and constraining policy choices. Such activities blur the boundary between war and peace and challenge traditional understandings of security (Caramancion et al., 2022).

The growing prominence of hybrid threats is closely linked to changes in the international system, particularly the intensification of competition between major powers. In the Euro-Atlantic context, these dynamics have exposed structural limitations of existing security frameworks. Institutions such as the European Union and NATO were designed to address clearly defined threats—economic instability in the case of the EU and military aggression in the case of NATO. Hybrid threats, however, deliberately exploit the space between these domains, where responsibilities overlap but coordination remains incomplete

*Corresponding author: ilija.zivotic@beopolis.edu.rs

(Kalniete & Pildegovics, 2021).

Since 2016, both organizations have developed responses to this challenge, but their approaches differ significantly. The European Union has focused on regulatory instruments, resilience-building, and the protection of democratic processes, particularly in the digital domain. Its response reflects its broader role as a normative and regulatory actor. NATO, by contrast, has approached hybrid threats primarily through the lens of security and defense, emphasizing intelligence integration, deterrence, and operational readiness (Balcaen et al., 2021).

Despite these efforts, the effectiveness of both approaches remains limited. One of the central problems is attribution. Hybrid operations are intentionally designed to obscure responsibility, often involving proxies, layered communication channels, and deniable infrastructures. This creates a structural dilemma: while political and legal responses require clear attribution, hybrid strategies are specifically constructed to prevent it (Caramancion et al., 2022).

At the same time, differences in institutional design further complicate the response. The EU operates through complex governance structures that require consensus among member states, which can slow decision-making. NATO, although also based on consensus, possesses more developed operational capabilities, allowing for faster responses in certain contexts. However, this advantage is offset by political constraints that limit the scope of collective action (Bajarūnas, 2020).

Technological developments add another layer of complexity. The expansion of digital platforms and data-driven communication has enabled hybrid campaigns to become more adaptive and scalable. As a result, hybrid threats are not static phenomena but evolving practices that continuously adjust to countermeasures (Caramancion et al., 2022).

Against this background, the central argument of this paper is that the current division of labor between the EU and NATO—often described as complementary—is insufficiently integrated to address hybrid threats effectively. The key issue is not the absence of tools, but the lack of strategic alignment and operational coordination between the two organizations.

Accordingly, this paper addresses two questions: how the EU and NATO operationalize their responses to hybrid threats, and what structural gaps limit their effectiveness. By focusing on practical implementation rather than formal strategies, the analysis aims to provide a more critical assessment of the Euro-Atlantic approach to hybrid threats.

2. EU AND NATO RESPONSES

The European Union has developed a layered and increasingly institutionalized approach to hybrid threats, centered on regulation, prevention, and societal resilience. Rather than relying on centralized operational capabilities, the EU's response is structured around governance instruments that aim to shape the environment in which hybrid activities occur. Platform governance has become a central mechanism through which the EU indirectly shapes the information environment in which hybrid threats operate (Gorwa, 2020). Key mechanisms include the Hybrid Fusion Cell, which enhances situational awareness through the aggregation of intelligence inputs, and the FIMI framework, which enables systematic identification of disinformation networks through behavioral and technical indicators (European External Action Service [EEAS], 2025). This reflects a broader shift toward analytical models that treat hybrid activity as a networked and adaptive phenomenon rather than a set of isolated incidents.

A concrete example of this approach can be observed in Moldova, where coordinated disinformation campaigns were designed to undermine public support for European integration. These campaigns relied on interconnected media ecosystems and amplification strategies across multiple digital platforms, demonstrating how hybrid threats exploit the openness of democratic information environments. Similar patterns have been identified in broader European contexts, where disinformation campaigns operate through hybrid media systems that combine traditional and digital channels (Bennett & Livingston, 2020).

At the regulatory level, the EU has significantly strengthened its capacity through instruments such as the Digital Services Act (DSA), which imposes obligations on large online platforms to assess and mitigate systemic risks related to disinformation and foreign interference. This regulatory approach reflects a distinctive strategic logic: instead of directly confronting hybrid actors, the EU seeks to constrain the infrastructures that enable their activities. Research shows that platform governance plays a critical role in shaping the dynamics of disinformation and hybrid influence operations (Gorwa, 2020).

However, this model also exposes structural limitations. The EU's reliance on coordination among member states and institutions often results in slower response times, particularly in rapidly evolving hybrid threat environments. The absence of centralized operational authority limits the Union's ability to translate situational awareness into immediate action, especially when responses require political

consensus or cross-sectoral alignment (Bajarūnas, 2020).

In contrast, NATO's approach is embedded in its security and defense mandate, enabling a more direct and operational posture. NATO integrates intelligence, military preparedness, and resilience-building into a unified framework, reflecting a strategic shift toward recognizing hybrid threats as a core security challenge. This shift is particularly visible in NATO's increasing emphasis on early warning, attribution, and coordinated response mechanisms.

Moreover, NATO benefits from more developed intelligence-sharing structures, which allow for faster information exchange and a reduced gap between detection and response. Empirical research on alliance behavior suggests that such integration enhances the ability to respond to complex and ambiguous threats, particularly when they span multiple domains (Kostyuk & Zhukov, 2017).

Nevertheless, NATO's operational advantage is not without constraints. Its effectiveness remains conditioned by political consensus among member states, which can delay or limit collective responses. This creates a structural tension between operational capability and political feasibility, which hybrid threat actors can exploit by operating below the threshold that would trigger a unified response.

3. NATO'S OPERATIONAL APPROACH TO HYBRID THREATS

NATO's approach to hybrid threats is characterized less by the introduction of entirely new instruments and more by the gradual integration of hybrid threat logic into its existing deterrence and defense architecture. Rather than treating hybrid threats as a separate category, NATO has incorporated them into its core strategic thinking, recognizing that contemporary conflict increasingly unfolds across interconnected domains, including cyber, informational, and conventional military environments.

A key feature of NATO's operational approach is the emphasis on intelligence integration and early warning. Hybrid threats are not addressed as isolated incidents, but as part of continuous adversarial activity designed to remain below the threshold of collective defense. This has led to the development of more structured analytical practices within the Alliance, aimed at reducing ambiguity and accelerating decision-making. As recent research shows, NATO's adaptation to hybrid threats has been driven by the need to improve responsiveness and strategic coherence in an environment where threats evolve faster than traditional decision-making cycles (Genini, 2025).

What distinguishes NATO from other actors is not only its analytical capacity, but its ability to directly translate intelligence into operational planning.Intelligence-sharing mechanisms within the Alliance reduce fragmentation and enable a more synchronized understanding of hybrid activity across member states. This is particularly important given that hybrid operations are inherently transnational, often targeting multiple states simultaneously through coordinated cyber, informational, and economic actions.

The case of Ukraine illustrates the multidimensional character of hybrid threats. Russian operations have combined cyberattacks, disinformation campaigns, and conventional military pressure in a mutually reinforcing manner. These actions demonstrate that hybrid warfare is not a substitute for conventional conflict, but rather a complementary layer that shapes the strategic environment before and during military engagement. NATO's response has therefore extended beyond traditional military support to include intelligence-sharing, cyber defense cooperation, and resilience-building measures across critical sectors.

At the same time, NATO has increasingly emphasized resilience as a core component of its hybrid threat strategy. This reflects a recognition that not all hybrid activities can be deterred or prevented; instead, reducing vulnerability and ensuring continuity of governance becomes a central objective. Recent discussions within NATO highlight the importance of societal resilience, critical infrastructure protection, and coordinated responses across civilian and military domains as key elements of this approach .

However, NATO's operational model also faces structural constraints. Its ability to act remains dependent on political consensus among member states, which can delay responses in rapidly evolving situations. Hybrid threat actors exploit this limitation by operating in the "grey zone," deliberately calibrating their actions to remain below the threshold that would trigger a unified response. This creates a persistent gap between detection and action, which remains one of the central challenges for NATO's adaptation to hybrid threats.

Ultimately, NATO's approach demonstrates a high degree of operationalization, particularly in intelligence integration and strategic awareness. Yet its effectiveness depends on its ability to reconcile rapid operational needs with inherently slower political decision-making processes—an imbalance that continues to define the Alliance's response to hybrid conflict.

4. DISCUSSION

The analysis of EU and NATO responses demonstrates that hybrid threats are not simply a new security challenge, but a structural feature of contemporary international relations that exposes systemic vulnerabilities within democratic systems. These vulnerabilities are particularly evident in the informational domain, where the openness of democratic societies creates opportunities for external manipulation. As recent studies suggest, disinformation campaigns are most effective not because of their content alone, but because they exploit pre-existing societal divisions and institutional weaknesses (Bennett & Livingston, 2018).

The case of Ukraine highlights the extent to which hybrid threats operate across multiple domains simultaneously. Cyber operations, disinformation campaigns, and conventional military actions are not separate tools but mutually reinforcing elements of a broader strategic approach. This convergence challenges traditional security models, which tend to treat threats as domain-specific. Instead, hybrid threats require cross-domain responses that integrate military, civilian, and technological capabilities.

In the Western Balkans, hybrid threats manifest differently but with similar strategic objectives. Rather than direct confrontation, influence operations focus on shaping public opinion, weakening institutional trust, and slowing down Euro-Atlantic integration processes. These dynamics illustrate that hybrid threats are context-dependent: while their tools may be similar, their effects vary depending on local political and social conditions.

A key insight emerging from this analysis is that both the EU and NATO are addressing different dimensions of the same problem, but without sufficient integration. The EU's regulatory and resilience-based approach is essential for addressing long-term vulnerabilities, particularly in the digital and informational space. NATO, on the other hand, provides the operational capacity needed to respond to immediate threats. However, the lack of synchronization between these approaches creates a strategic gap that hybrid threat actors can exploit. This misalignment does not merely reduce efficiency—it creates structural opportunities for hybrid threat actors to exploit gaps between institutional mandates.

Another critical issue is the problem of attribution. As hybrid operations are deliberately designed to obscure responsibility, both organizations face significant constraints in responding effectively. Attribution is not merely a technical challenge but also a political one, as responses require consensus among actors with differing threat perceptions and strategic priorities. Research indicates that uncertainty in attribution often leads to delayed or diluted responses, reducing their deterrent effect (Lindsay, 2020).

Technological developments further intensify these challenges. The increasing use of artificial intelligence in information operations allows for the rapid generation and dissemination of tailored content, significantly enhancing the scale and precision of disinformation campaigns. This evolution indicates that hybrid threats are becoming progressively more adaptive and capable of circumventing existing detection frameworks, which necessitates continuous innovation in both analytical tools and policy responses (Olawunmi, 2025).

Importantly, hybrid threats challenge not only security institutions but also the conceptual foundations of security policy. The distinction between internal and external security becomes increasingly blurred, as many hybrid activities target domestic political processes while being orchestrated externally. This raises questions about the adequacy of existing institutional frameworks, which are often based on a clear separation between these domains.

Ultimately, the findings suggest that the effectiveness of EU and NATO responses depends less on the development of new instruments and more on their ability to integrate existing ones. Without deeper coordination, shared analytical frameworks, and improved attribution mechanisms, hybrid threats will continue to exploit institutional fragmentation.

5. CONCLUSION

This paper has examined how the European Union and NATO operationalize their responses to hybrid threats and has demonstrated that, despite significant progress since 2016, important structural limitations remain. Hybrid threats are not simply a category of security challenges but a persistent mode of strategic competition that exploits the institutional and societal characteristics of democratic systems. As such, they cannot be effectively addressed through traditional, domain-specific approaches.

The analysis has shown that the EU and NATO operate according to different but complementary strategic logics. The EU focuses on regulation, resilience, and the governance of digital and informational environments, addressing the structural conditions that enable hybrid threats. NATO, in contrast, provides operational capabilities, particularly in intelligence integration, deterrence, and rapid response. However,

this division of labor remains insufficiently integrated in practice.

Two key limitations stand out. First, the problem of attribution continues to constrain both organizations. Without timely and credible attribution, political and strategic responses remain limited, reducing their deterrent effect. Second, coordination between the EU and NATO remains uneven. Despite formal cooperation frameworks, differences in institutional design and decision-making processes hinder the development of fully synchronized responses.

These findings suggest that the effectiveness of the Euro-Atlantic response to hybrid threats depends less on the creation of new instruments and more on the integration of existing ones. In this context, three policy implications emerge. First, the development of a joint EU–NATO attribution framework would strengthen the credibility and timeliness of responses. Second, the establishment of shared analytical standards—particularly in the identification and assessment of hybrid activities—would reduce fragmentation and improve interoperability. Third, deeper operational coordination, including joint exercises and information-sharing mechanisms, is necessary to bridge the gap between prevention and response.

Ultimately, hybrid threats challenge not only the capabilities of institutions but also their ability to act collectively under conditions of uncertainty and ambiguity. Addressing this challenge requires a shift from parallel approaches toward genuinely integrated strategies, capable of responding to hybrid threats as a systemic and evolving feature of contemporary security. In this sense, hybrid threats should be understood not as an exception, but as the defining condition of contemporary security.

REFERENCES

Bajarūnas, E. (2020). Addressing hybrid threats: Priorities for the EU in 2020 and beyond. European View, 19(1), 62–70. https://doi.org/10.1177/1781685820912041

Balcaen, P., Du Bois, C., & Buts, C. (2021). Sharing the burden of hybrid threats: Lessons from the economics of alliances. Defence and Peace Economics, 34(2), 142–159. https://doi.org/10.1080/10242694.2021.1991128

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication, 33(2), 122–139. https://doi.org/10.1177/0267323118760317

Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum. Data, 7(4), 49. https://doi.org/10.3390/data7040049

European Centre of Excellence for Countering Hybrid Threats. (2024). Hybrid threats as a concept. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

European External Action Service. (2025). 3rd EEAS report on foreign information manipulation and interference (FIMI). https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. New Perspectives, 33(2), 122–149. https://doi.org/10.1177/2336825X251322719

Gorwa, R. (2020). What is platform governance? Information, Communication & Society, 23(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Kalniete, S., & Pildegovics, T. (2021). Strengthening the EU's resilience to hybrid threats. European View, 20(1), 23–33. https://doi.org/10.1177/17816858211004648

Kostyuk, N., & Zhukov, (2017). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?. Journal of Conflict Resolution. No.63. DOI:10.1177/0022002717737138

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Mansoor, P. R., & Murray, W. (2012). Hybrid warfare: Fighting complex opponents. Cambridge University Press. https://assets.cambridge.org/97811070/26087/frontmatter/9781107026087_frontmatter.pdf

Olawunmi, K. (2025). Computational propaganda, disinformation, and democracy: Multidisciplinary strategies for 2025. International Journal of Social Science and Human Research. https://doi.org/10.47191/ijsshr/v8-i9-19