IE University IE International Policy Review (IPR)
Journal **7 Issue 1** (2026)
https://ipr.blogs.ie.edu/

Responding to Hybrid Threats: Coordinating NATO, EU, and U.S. Strategies in the Era of Gray-Zone Competition

Martina Magrini

Department of Political and Social Sciences, University of Bologna, Forlì, Italy.
Master's Degree in International Relations and Diplomatic Affairs.

E-mail: martina.magrini6@studio.unibo.it

Published January 2026

Editor: Gabriela Vargas Hernandez, IE University.

Abstract

This article analyses how NATO, the European Union and the United States address hybrid threats and assesses the effectiveness of coordinating their approaches, through an analysis of the Baltic Sea and Black Sea regions. Although each actor adopts its own distinct framework – NATO focused on collective defence, the European Union on civil and regulatory resilience, and the United States on integrated deterrence – their strategies are gradually converging in response to growing hybrid pressure from authoritarian actors.

While the Baltic region demonstrates how the integration of a coordinated military presence, integrated intelligence sharing and strong social resilience can produce an effective hybrid deterrence strategy, the Black Sea, on the contrary, highlights persistent shortcomings such as fragmented coordination, uneven infrastructure and mobility, and limited integration of military and civilian instruments.

The analysis of the two case studies highlighted that, despite significant progress, transatlantic hybrid deterrence is still limited by overlapping mandates, inadequate information sharing and shortcomings in critical infrastructure protection. The article concludes with a series of recommendations, such as improving operational thresholds, enhancing joint situational awareness, and promoting more integrated interregional planning, which are considered essential for achieving consistent and effective transatlantic hybrid deterrence.

Keywords: hybrid threats, hybrid deterrence, grey-zone operations, NATO–EU–US cooperation, Baltic and Black Sea security.

1. Introduction

Hybrid threats have become the defining feature of twenty-first-century conflict, blurring the line between war and peace and testing the credibility of transatlantic security institutions. Originally conceptualised by Frank Hoffman (2007), hybrid warfare refers to the conjunction of conventional military force, irregular tactics, cyber-warfare, and informational operations on one field of conflict. This allows state and non-state actors to exploit an adversary's political and social weaknesses without being

committed to a combat engagement.[1] Likewise, NATO (2024) defines hybrid threats, as the synchronized exploitation of military and non-military means – such as cyberattacks, disinformation campaigns, and economic pressure – to destabilize open societies "below the level of armed conflict".[2] Taken together, these views help to explain why hybrid operations have taken on a new prominence in transatlantic security, prompting NATO, the European Union (EU) and the United States to reimagine how deterrence and resilience are constructed in this century.

Hybrid strategies have profoundly reshaped Europe's security landscape. The effects of Russia's cyber campaign against Estonia in 2007, the annexation of Crimea in 2014, and full-scale invasion of Ukraine in 2022 provide examples of how grey-zone operations combine military pressure with disinformation and economic coercion to erode regional stability.[3] With a primary focus on security on land, this article analyses how hybrid threats undermine Eastern European territorial stability and allied deterrence. Their impact is most visible in the Baltic and Black Sea regions, where political, military and societal vulnerabilities converge and have turned both theatres into testing grounds for hybrid deterrence.

Although the United States, NATO and the European Union have expanded coordination and resilience efforts since 2014, the effectiveness of these mechanisms remains contested.[4] This article therefore analyses how these actors respond to hybrid threats on Europe's eastern flank, and examines whether they are moving from parallel approaches toward a genuinely integrated hybrid deterrence architecture. In order to compare institutional and regional dynamics across various forms of coordination and strategic gaps, the analysis uses a qualitative comparative approach. The paper concludes that, while cooperation has improved since 2014, enduring gaps between military and civilian tools continues to limit the coherence of the transatlantic response.

2. Background

The concept of hybrid warfare emerged in the early 2000s to capture the increasing fusion of different modes of conflict within a complex and fluid battlespace. Frank Hoffman (2007) characterised this transformation as the "blurring of modes of war", in which states and non-state actors combine conventional capabilities, irregular strategies, terrorism, and criminal activities within a single operational setting to generate synergistic effects. The analysis of the 2006 conflict between Israel and Hezbollah offered the first empirical demonstration of this approach, showing how a non-state actor could integrate state-level

[1] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 8.

[2] NATO, "Hybrid Threats," NATO Official Portal, last updated 2024.

[3] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015), 5–6.

[4] NATO, "Cyber Defence Overview," last updated March 2023; Chatham House, *Hybrid Warfare in Europe: Lessons from Ukraine* (London: Chatham House, 2022); CSIS, *Resilience in the Gray Zone* (Washington, DC: Center for Strategic and International Studies, 2022).

weaponry, decentralised networks and urban guerrilla tactics to challenge a conventional military force.[5] This theoretical foundation provided the basis for the subsequent understanding of hybrid warfare in the Euro-Atlantic context, especially after Russia began employing similar tactics in its neighbourhood from 2007 onwards.

Building on Hoffman's formulation, Michael J. Mazarr broadened the analytical scope by situating hybrid warfare within the wider framework of grey-zone competition, coercive action conducted below the threshold of open warfare and characterised by ambiguity, gradualism and deniability. In this "space between peace and war", revisionist powers such as Russia and China pursue incremental change through strategic gradualism, understood as a sequence of small cumulative actions designed to alter the status quo without provoking direct military escalation. Mazarr argues that actors increasingly rely on non-military instruments such as economic coercion, cyber operations, and disinformation campaigns to erode adversaries' cohesion.[6]

Russia's cyberattack on Estonia in 2007 and its annexation of Crimea in 2014 prompted the Euro-Atlantic community to recognise hybrid threats as a structural challenge. These events demonstrated how strategic effects traditionally associated with war could be produced by non-kinetic means. In response to these threats, NATO has adopted a new doctrine that includes the introduction of hybrid warfare as a response tool. An important step forward in recognising the interdisciplinary nature of these issues was marked by the establishment of the European Centre of Excellence for Countering Hybrid Threats in Helsinki in 2017.[7] Disinformation, cyber-attacks and energy coercion are examples of hybrid operations that NATO's 2022 Strategic Concept specifically describes as tools aimed at "destabilising societies below the level of armed conflict".[8]

In a similar vein, the European Union has developed its own Joint Framework on Countering Hybrid Threats (2016) and its more recent NATO–EU Joint Declaration on Cooperation (2023), with the aim of reconciling military resilience with civilian resilience.[9] Despite NATO's potential to project military might, the EU's strength lies in its regulatory and normative instruments, including cyber governance, energy diversification, and strategic communication. The primary issue is that of achieving synchronisation: the question of how to align the concept of deterrence as espoused by NATO with that of resilience as promoted by the EU, within the context of a coherent transatlantic framework.

[5] Hoffman, *Conflict in the 21st Century*, 14–35.
[6] Mazarr, *Mastering the Gray Zone*, 1–8.
[7] European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2023* (Helsinki: Hybrid CoE, 2023).
[8] North Atlantic Treaty Organization (NATO), Strategic Concept 2022 (Madrid: NATO, 2022).
[9] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint Framework on Countering Hybrid Threats: A European Union Response (Brussels: European External Action Service, 2016); European Union and North Atlantic Treaty Organization (NATO), Joint Declaration on EU–NATO Cooperation (Brussels: European External Action Service, 2023).

The United States, as the central pillar of the transatlantic alliance, has also reframed its strategic outlook around hybrid threats. The 2022 National Defense Strategy defines the "integration of military and non-military tools" as essential to deterrence by denial, highlighting cyber resilience and information integrity as key domains of competition.[10] American strategic documents increasingly converge with European approaches in identifying hybrid coercion as the principal mechanism through which authoritarian states attempt to erode Western unity without triggering collective defence.

Empirically, the hybrid threat space is most apparent on the eastern border of Europe. The Baltic nations have been targeted with persistent cyberattacks, disinformation campaigns and political subversion since 2007; the Black Sea region has served as a testing ground for Russia's hybrid playbook, one that pairs military intimidation with economic pressure and digital manipulation.[11] The annexation of Crimea in 2014 and the full-scale invasion of Ukraine in 2022 illustrate how grey-zone operations can escalate into open warfare. As Bettina Renz observes, Russia's employment of these hybrid instruments does not necessarily indicate a novel mode of warfare but rather signifies a strategic spectrum wherein non-kinetic tools function as the foundational framework and enabler of kinetic operations.[12]

Despite growing awareness, significant conceptual and operational gaps remain. Scholars such as Katri Pynnöniemi and András Rácz underline the lack of a shared definition of hybrid warfare among NATO and EU actors, which complicates coordination.[13] Moreover, the transatlantic response continues to be fragmented along the civil–military divide: NATO retains primary responsibility for defence, while the EU focuses on resilience and regulation. This division of labour, while logical, risks producing incoherence in crisis scenarios that require simultaneous political, informational, and military responses.

Taken together, these dynamics suggest that hybrid threats have catalysed an ongoing redefinition of deterrence and resilience in the Euro-Atlantic security order. The next section will examine how these institutional frameworks operate in practice in the Baltic and Black Sea regions, evaluating whether the transatlantic community is evolving from ad-hoc cooperation toward a genuinely integrated hybrid deterrence architecture.

[10] U.S. Department of Defense, *National Defense Strategy of the United States of America: 2022* (Washington, D.C.: U.S. Government Publishing Office, 2022).

[11] Keir Giles, Russia's New Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power (London: The Royal Institute of International Affairs, Chatham House, 2016).

[12] Bettina Renz, Russia's Military Revival (Cambridge: Polity Press, 2018), 122–125.

[13] Katri Pynnöniemi and András Rácz, Russia's Hybrid Warfare: A New Challenge for Europe and the Atlantic Alliance, FIIA Report 45 (Helsinki: Finnish Institute of International Affairs, 2016), 5–8, 78–80.

3. Analysis

3.1 NATO's Approach

NATO's approach to hybrid threats has evolved significantly since their formal recognition at the 2014 Wales Summit, where Allies acknowledged that adversaries could combine military, paramilitary and civilian instruments in coordinated campaigns below the threshold of open war.[14] The 2016 Warsaw Summit built on this assessment by adopting a dedicated strategy and implementation plans to address hybrid challenges. It also clarified that the primary responsibility for countering hybrid threats lies with the affected Ally, while NATO provides support at all stages of a hybrid campaign and, in extreme cases, may treat a severe hybrid attack as an armed attack under Article 5 of the Washington Treaty.[15]

The 2022 Strategic Concept identifies authoritarian actors that interfere with democratic processes and institutions as key sources of hybrid risk. It commits the Alliance to strengthening preparedness, deterrence and protection against political, economic, energy and information tools used to coerce Allies, whether directly or through proxies. The Concept emphasises the need to support partners in countering hybrid challenges and to deepen cooperation with actors such as the European Union, whose civilian instruments complement NATO's military capabilities in a cross-domain hybrid environment.[16]

Operationally, NATO has enhanced its ability to detect and respond to hybrid campaigns by strengthening intelligence fusion, information-sharing and early warning, and by acting as a hub for training, exercises and expertise on hybrid threats. It seeks to deter hybrid attacks by increasing the readiness and adaptability of Allied forces and by expanding its toolkit for responding to disruptions in cyberspace, critical infrastructure and the information domain.[17] Yet despite these advances, NATO's approach remains primarily state-centric and defence-oriented: it depends on national capacities for the initial response, resulting in uneven levels of resilience across the Alliance. Moreover, the threshold at which hybrid activity could trigger collective defence remains ambiguous, a tension that is particularly salient in frontline regions such as the Baltic and Black Sea areas.

3.2 EU's Approach

Rather than relying on military deterrence, the European Union frames hybrid warfare as a multidimensional challenge requiring an integrated and predominantly civilian response. The 2016 Joint Framework on Countering Hybrid Threats sets out measures to strengthen resilience at the national, EU and partner levels. It emphasises improved situational awareness through enhanced information-exchange mechanisms, coordinated strategic communication, and the establishment of the EU Hybrid Fusion Cell within the European Union Intelligence and Situation Centre (EU INTCEN), which is tasked with analysing both classified

[14] NATO, "Wales Summit Declaration," September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
[15] NATO, "Warsaw Summit Communiqué," July 9, 2016.
[16] NATO, *Strategic Concept 2022*.
[17] NATO, "Countering Hybrid Threats," last modified 2024.

and open-source data on hybrid threats. The Framework also outlines initiatives to bolster resilience in cybersecurity, critical infrastructure, financial systems and the prevention of radicalisation, while calling for deeper coordination with NATO to address hybrid threats jointly.[18]

Building on this foundation, the 2022 Strategic Compass seeks to consolidate the EU's role as a "resilience provider" by developing the EU Hybrid Toolbox. This toolkit brings together existing and emerging instruments, including the creation of hybrid rapid response teams, to support Member States, CSDP missions and partner countries facing hybrid campaigns.[19] Taken together, these measures highlight the EU's distinct contribution to hybrid deterrence: mobilising regulatory, economic and informational tools that complement NATO's military posture.

The 2023 EU–NATO Joint Declaration reinforces this dual-track approach by affirming the organisations' complementary roles in countering hybrid and cyber threats, enhancing military mobility and protecting critical infrastructure.[20] Yet structural disparities persist. The division of labour between NATO's defence orientation and the EU's civilian competences, combined with overlapping mandates and uneven national capacities, continues to inhibit the development of a fully integrated hybrid deterrence architecture, a gap with significant implications for transatlantic cohesion.

3.3 U.S. Approach

The 2022 National Defense Strategy places hybrid and grey-zone challenges at the core of U.S. strategic planning. It underscores that competitors seek to erode the status quo through coercive actions that stay short of overt armed confrontation, frequently relying on proxies, cyber capabilities and emerging technologies to complicate attribution and impose incremental costs on the United States and its allies. These dynamics reinforce Washington's view that hybrid competition demands a whole-of-government approach rather than a solely military response.

To address this environment, the Strategy advances the concept of integrated deterrence, defined as the coordinated use of military, diplomatic, informational, economic and technological instruments across domains, theatres and allied networks.[21] Integrated deterrence combines reactive and proactive elements: the United States must respond credibly to hybrid pressures in key regions while also operating in the grey zone to shape competitors' behaviour before escalation occurs. This approach relies on a broad set of tools, including Special Operations Forces, theatre security cooperation, intelligence assets and interagency coordination with departments such as State, Treasury and Commerce as well

[18] European Commission, Joint Framework on Countering Hybrid Threats: A European Union Response (Brussels: European Commission, 2016).

[19] Council of the European Union, A Strategic Compass for Security and Defence (Brussels: Council of the EU, 2022).

[20] European Council. EU–NATO Joint Declaration on Cooperation. Brussels: European Council, January 10, 2023.

[21] U.S. Department of Defense, National Defense Strategy of the United States of America 2022, including the Nuclear Posture Review and Missile Defense Review (Washington, D.C.: Department of Defense, 2022), 1–16.

as strong partnerships with allies, notably NATO and the Five Eyes.[22]

Collectively, these measures reflect a growing convergence between U.S., NATO and EU strategies, particularly in their shared emphasis on cross-domain coordination and resilience. Yet important differences remain: Washington's global posture and its reliance on hard-power assets distinguish its approach from the EU's civilian focus and NATO's collective-defence mandate. Nevertheless, the U.S. commitment to integrated deterrence reinforces transatlantic efforts to manage hybrid threats more coherently, an alignment especially relevant in vulnerable theatres such as the Baltic and Black Sea regions.

3.4 Comparative Assessment

The European Union, NATO, and the United States have each developed distinct yet increasingly convergent approaches to hybrid threats. Despite institutional differences, all three actors conceptualise hybrid warfare as a multidimensional challenge requiring resilience, preparedness, and coordinated deterrence. NATO remains the central military actor, relying on collective defence mechanisms and the rapid deployment of forces to deter hybrid aggression. Its strength lies in operational capacity and in integrating military and intelligence tools within a common security framework. The European Union complements this approach through its extensive civilian and regulatory instruments, including the Hybrid Fusion Cell and the Hybrid Toolbox, which enhance situational awareness, resilience, and policy coordination across Member States.[23] Meanwhile, the United States adopts a global strategy of integrated deterrence, linking military, diplomatic, economic, and technological instruments to address hybrid and grey-zone threats worldwide, while strengthening partnerships with NATO and the EU.[24]

Yet, despite this growing conceptual alignment, institutional asymmetries and overlapping competences continue to limit strategic coherence. Coordination often occurs through ad hoc political consultations rather than permanent operational frameworks, which constrains collective responses to complex hybrid campaigns. These structural gaps become particularly evident in regions of heightened hybrid activity, such as the Baltic and the Black Sea areas, where differing priorities and capacities among allies expose the limits of current coordination mechanisms. Examining these regional cases provides a concrete illustration of how the transatlantic partnership performs under pressure and reveals the practical obstacles that still prevent the full operationalisation of an integrated hybrid deterrence system.

3.5 Case studies

The assessment of transatlantic hybrid deterrence effectiveness requires observing its operational outcomes in particular regional environments. The Baltic and Black Sea regions serve as primary examples because they face

[22] Atlantic Council, "The Pentagon's Focus on the Gray Zone," Scowcroft Center for Strategy and Security, Gray Zone Task Force, December 13, 2022.

[23] European Commission, Joint Framework on Countering Hybrid Threats.

[24] U.S. Department of Defense, National Defense Strategy 2022.

ongoing political, military and informational threats, yet maintain different levels of institutional unity, defensive strength and strategic risk exposure. The Baltic region serves as an example of NATO, EU and United States military, cyber and informational coordination against repeated hybrid attacks. The Black Sea operates as a multifaceted unstable environment shaped by the 2014 annexation of Crimea and the ongoing war in Ukraine. The two cases offer essential insight into how transatlantic actors modify their hybrid deterrence approaches when dealing with different territorial and operational settings.

3.5.1 Baltic Region: A Model of Effective Hybrid Deterrence

The Baltic region has long been at the frontline of hybrid confrontation, where Russia's multidimensional pressure campaigns have turned it into a laboratory for transatlantic deterrence and resilience. Geographic proximity to Russia and Belarus, combined with demographic and informational vulnerabilities, creates conditions that Moscow systematically exploits. Since 2014, Russia has coordinated an integrated mix of cyber operations, disinformation, energy coercion, and border provocations to test NATO's cohesion and undermine democratic resilience. According to the Hybrid Centre of Excellence, these activities have evolved from sporadic influence operations into a structured hybrid strategy aimed at eroding societal trust and Western unity through disinformation, agents of influence, cyberattacks, psychological manipulation, physical sabotage and the weaponisation of migration.[25]

NATO's response has centred on deterrence by presence and enhanced situational awareness. The Enhanced Forward Presence (eFP), established following the 2016 Warsaw Summit, deployed four multinational battlegroups to Estonia, Latvia, Lithuania, and Poland by 2017, demonstrating the Alliance's commitment to collective defence under Article 5. A complementary Tailored Forward Presence (tFP) was developed in Bulgaria and Romania to reinforce posture in the southeast. After Russia's full-scale invasion of Ukraine in 2022, NATO expanded this framework by creating four additional battlegroups in Bulgaria, Hungary, Romania, and Slovakia, now consolidated as the Forward Land Forces, the cornerstone of the Alliance's strengthened forward defence. These units operate in close integration with NATO's Integrated Air and Missile Defence network and maritime vigilance initiatives such as Baltic Sentry, which focuses on critical undersea infrastructure and Eastern Sentry, a multi-domain operation strengthening deterrence along the entire eastern flank.[26] Together, these developments reflect NATO's assessment of Russia as "the most significant and direct threat to Euro-Atlantic security" and illustrate the shift from deterrence by presence toward persistent, multi-domain deterrence across land, air, maritime, cyber and space.[27]

[25] Hybrid Centre of Excellence, Russia's Hybrid Threat Tactics against the Baltic Sea Region (Helsinki: Hybrid CoE, 2024).
[26] NATO, "Strengthening NATO's Eastern Flank," last updated October 23, 2025.
[27] NATO, *Strategic Concept 2022*, 4.

In addition to this stance, the United States has played a central supporting role through the deployment of rotational troops, joint training exercises and intelligence-sharing efforts organised by U.S. European Command (EUCOM). The 2023 EUCOM Posture Statement designates the Baltic region as a strategic priority, emphasizing that deterrence and assurance along NATO's eastern flank rely on integrated joint capabilities, forward-deployed forces, and close interoperability with Allied militaries. To this end, Washington has strengthened defence cooperation with frontline NATO members, most notably Poland and the Baltic States, through prepositioned equipment, improved training and the establishment of the U.S. Army V Corps forward headquarters in Poznań as permanent command node. These efforts complement NATO's Enhanced Forward Presence by providing additional enabling assets, particularly in logistics, air defence, and intelligence domains.[28]

While NATO and the United States concentrate primarily on military deterrence, the European Union has developed a complementary framework centred on societal and informational resilience. The European External Action Service established the East StratCom Task Force in 2015 to counter disinformation campaigns targeting Baltic societies by providing coordinated strategic communication. Initially composed of three staff members, East StratCom now operates with sixteen full-time specialists monitoring media in more than twenty languages and managing the EUvsDisinfo database, which documents thousands of cases of pro-Kremlin disinformation. The task force also delivers training programs to partner-state officials, supports independent journalism and enhances public awareness of EU policies across the Eastern Partnership region.[29] Concurrently, the EU Cybersecurity Strategy for the Digital Decade strengthens the protection of critical infrastructure and promotes regional cooperation on cyber capacity-building, reinforcing the broader resilience architecture on which Baltic defence depends.[30]

The EU and NATO have developed strategic communication cooperation that has become essential for their operations in the Baltic region through the collaboration between the EU's East StratCom unit and the NATO Strategic Communications Centre of Excellence based in Riga. The partnership enables knowledge sharing between the two organisations and enables the creation of coordinated messaging to counter hybrid interference through coordinated action in the cyber and information domains.[31] These efforts demonstrate that the EU's resilience tools effectively

[28] U.S. European Command, Statement of Gen. Christopher G. Cavoli, U.S. European Command, to the House Armed Services Committee, 26 April 2023, 6–7.

[29] European Parliament, Background Note, Session I: Protection and Securing the European Union — Hybrid Threats as an External Factor Destabilising Europe (Brussels: European Parliament, 19 March 2024), 3–4.

[30] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, December 16, 2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

[31] European Parliament, Background Note, Session I, 4.

support NATO's deterrence strategy, improving the Baltic states' ability to withstand and recover from hybrid threats.

3.5.2 Black Sea Region: A Fragmented Hybrid Deterrence Environment

Russia has long viewed the Black Sea as a strategic anchor of its great-power status and a core platform for projecting influence across the Mediterranean, the Middle East and Africa. Following the illegal annexation of Crimea in 2014, Moscow consolidated a dense anti-access/area denial (A2/AD) architecture that enables its forces to control much of the basin and shape the regional security environment. Yet this military build-up represents only one dimension of a broader hybrid strategy. Russia systematically employs grey-zone tactics, including disinformation, energy leverage and strategic corruption, to advance its objectives while maintaining plausible deniability and avoiding overt escalation with neighbouring states or the NATO Alliance. These tools are designed to disrupt political systems, weaken state resilience and constrain the ability of regional actors to respond to mounting Russian pressure.[32]

NATO's strategic posture in the Black Sea has transformed significantly since Russia's full-scale invasion of Ukraine in 2022. The war exposed the region as a critical fault line in Euro-Atlantic security and generated new consensus among Allies on the need to strengthen the southeastern flank. In line with the 2022 Strategic Concept, NATO established new multinational battlegroups in Romania and Bulgaria, supported by France and Italy, and expanded regional readiness through enhanced air and missile defence assets, intelligence cooperation and improved mobility corridors. However, maritime constraints persist due to Türkiye's implementation of the Montreux Convention, which limits the access of non-littoral Allied warships. The 2023 Vilnius Summit formally recognised the Black Sea's strategic importance, endorsed new regional defence plans and higher readiness targets, and reaffirmed Allied commitments to regional security, freedom of navigation and situational awareness. It also intensified support for Ukraine's naval modernisation and expanded tailored assistance to partners such as Moldova and Georgia, integrating them more closely into the Euro-Atlantic security framework.[33]

The United States frames the Black Sea as a key arena in its long-term competition with Russia and China, viewing regional stability as essential to Euro-Atlantic security. The Department of State has presented its 2023 Strategy for Security in the Black Sea Region which demonstrates Washington's commitment to establishing a secure, interconnected and prosperous region, free from any coercive or malign influence. The strategy combines military, diplomatic and economic instruments to support coastal Allies such as Romania and Bulgaria, while strengthening ties with Türkiye and providing defence aid and political support to Ukraine, Georgia and Moldova. It is structured around five connected elements which

[32] NATO Parliamentary Assembly, Black Sea Security Report (Brussels: NATO PA, 2023), 6–7.

[33] NATO Parliamentary Assembly, Black Sea Security Report, 11–14.

include political engagement, security cooperation, economic and energy resilience and democratic governance all pursued in collaboration with NATO and the European Union. The Three Seas and Bucharest Nine formats serve as programs which enhance regional connectivity while the Global Engagement Centre operates multiple initiatives to combat Russian disinformation and corrupt activities. The established measures demonstrate Washington's intention to implement hard and hybrid deterrence strategies thus reinforcing NATO's posture and supporting long-term stability across the Black Sea.[34]

The European Union has reframed its engagement in the Black Sea around a comprehensive policy approach that links security, resilience, and prosperity as mutually reinforcing pillars. The EU Strategic Approach to the Black Sea Region (2024) sets out a three-pillar framework aimed at enhancing security and stability, fostering sustainable economic development, and promoting environmental protection and resilience. In contrast with previous initiatives such as the 2007 Black Sea Synergy, the new strategy embeds a stronger security dimension across all policy areas, recognising that maritime security, freedom of navigation and the protection of critical infrastructure are essential to regional stability and connectivity. Its flagship initiative, the Black Sea Maritime Security Hub, integrates EU and partner contributions to improve situational awareness, demining, coast-guard cooperation and the protection of maritime infrastructure through advanced monitoring technologies and coordinated civil–military arrangements.[35]

Within this framework, the EU recognises that the Black Sea has become a primary target of hybrid operations, including cyberattacks, foreign information manipulation and interference (FIMI), and other disruptive actions. To address these threats, the Joint Communication on the EU's Strategic Approach to the Black Sea Region introduces a hybrid-threat agenda focused on reinforcing national and societal resilience. It promotes joint response networks to counter disinformation, particularly in rural and border areas, and calls for enhanced coordination and information-sharing on cyber and hybrid threats affecting critical infrastructure. These actions build on the Hybrid Risk Survey, CSDP Missions in the region (such as EUPM Moldova) and the EU Hybrid Rapid Response Teams, implemented in coordination with NATO and other like-minded partners.

The EU also commits to imposing costs on malign actors through diplomatic measures, public attributions, and sanctions, leveraging its Hybrid, Cyber, and FIMI Toolboxes. It supports partners' capacities through the use of AI and digital technologies to counter disinformation, while promoting media literacy, fact-checking cooperation, and critical thinking to strengthen democratic resilience. Multi-stakeholder mechanisms enhance online accountability and the protection of fundamental rights in the digital sphere. Collectively, these initiatives form a

[34] U.S. Department of State, Strategy for Security in the Black Sea Region (Washington, DC: U.S. Government Printing Office, 2023), 26–33.

[35] European External Action Service (EEAS), EU Strategic Approach to the Black Sea Region, last updated March 11, 2024.

layered model of hybrid deterrence grounded in close cooperation with NATO and regional partners. By integrating diplomatic, technological, and societal instruments, the EU consolidates its role as a hybrid security provider in the eastern neighbourhood, a dynamic whose effectiveness becomes clearer when contrasted with developments in the Baltic region.[36]

The comparative examination of the Baltic and Black Sea regions shows that, although transatlantic hybrid deterrence has moved toward greater operational integration, significant asymmetries persist across regional theatres. The two cases highlight both the progress made in NATO–EU–US coordination and the structural, political and capability gaps that still limit the emergence of a coherent, fully integrated hybrid deterrence architecture. These findings provide the foundation for reassessing the main strategic challenges and identifying the policy adjustments required to strengthen transatlantic responses to hybrid threats.

4. Policy Analysis/Recommendation

Despite the extensive coordination mechanisms developed across the transatlantic community and the significant progress achieved in the Baltic and Black Sea regions, substantial coordination gaps remain within the collective response to hybrid threats. Both cases demonstrate that the success of deterrence efforts does not automatically translate into seamless institutional integration. In practice, overlapping mandates, asymmetric resource allocations, and limited information exchange continue to undermine the efficiency of transatlantic cooperation.

4.1 Baltic Region: Operational Gaps

Although the Baltic region represents the most advanced arena of NATO–EU–U.S. hybrid deterrence coordination, several gaps persist beneath its apparent success. Recent analyses underline that the very need for "far-reaching consolidation of activities and cross-border cooperation between institutions" indicates that coordination among armed forces, coast guards, and intelligence agencies of coastal states remains incomplete.[37] The absence of unified data-sharing frameworks limits the development of a common situational awareness system, hampering early detection and joint response to maritime incidents. This issue extends to the technological domain: while modern tools such as autonomous monitoring systems and artificial intelligence are increasingly deployed to track non-reporting vessels and potential hybrid activities, their integration into a shared operational picture across national systems remains partial and uneven across national systems.

These deficiencies further affect the protection of critical infrastructure (CI), where vulnerabilities at sea translate directly into risks on land. Energy terminals,

[36] European Commission and High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament and the Council: The European Union's Strategic Approach to the Black Sea Region. JOIN (2025) 135 final. Brussels, 28 May 2025.

[37] Rafał Miętkiewicz, "Hybrid Threats in the Baltic Sea: The Results of Analysis of Countermeasure Options," *Scientific Journal of the Polish Naval Academy* 234, no. 3 (2023): 58–61.

undersea cables, and cross-border pipelines are connected to terrestrial networks that remain unevenly secured and governed by different regulatory logics. As the report notes, "sharing sensitive knowledge can be resented by the private sector," revealing persistent trust and communication deficits between national security institutions and energy-industry stakeholders.[38] These weaknesses became evident during the 2024 Balticconnector incident, when repair operations required nearly six months due to the absence of a joint rapid-response and cross-border repair mechanism, disrupting not only maritime flows but also domestic energy resilience in Finland and Estonia.

Another structural limitation concerns the misalignment between NATO operational standards and EU regulatory instruments. While the Revised EU Maritime Security Strategy and the Critical Entities Resilience Directive establish shared principles for maritime and infrastructural security, their implementation remains nationally fragmented and poorly integrated with NATO's resilience frameworks.[39] The result is a hybrid security landscape that is technologically advanced but institutionally disjointed, one where deterrence functions through presence and vigilance, yet coordination gaps in legal, informational, and technological domains continue to erode collective efficiency.[40]

4.2 Black Sea Region: Operational Gaps

While the Black Sea Region has increasingly become a focal point of Euro-Atlantic security since 2022, transatlantic coordination there remains far less cohesive than in the Baltic theatre. Analyses of the region underline that, despite NATO's reinforced presence and the European Union's growing engagement, the overall approach "requires a more comprehensive and unified strategy" to effectively counter hybrid threats.[41]

A first gap stems from the absence of an integrated framework linking NATO, the EU, and the United States. Although the 2022 Strategic Concept recognized the Black Sea's strategic importance, Allies have yet to translate this into a joint operational plan. As Lord Mark Lancaster noted in his 2023 report, commitments made in Vilnius remain largely declaratory until shaped into a collective strategy defining clear priorities and responsibilities. The United States has advanced its own Black Sea Security Act, but coordination with NATO and EU initiatives remains fragmented, resulting in overlapping mandates and limited synergy.[42]

A second gap concerns insufficient coordination on land security and mobility across the southeastern flank. NATO's new battlegroups in Romania and Bulgaria lack the degree of logistical integration seen in the Baltic region.

[38] Miętkiewicz, "Hybrid Threats in the Baltic Sea," 60.

[39] European Union, Revised EU Maritime Security Strategy (Brussels: European External Action Service, 2023).

[40] NATO, Hybrid Threats and Hybrid Warfare: Resilience in Practice (Brussels: NATO Strategic Communications Centre of Excellence, 2024); European Union, Directive (EU) 2023/1230 on the Resilience of Critical Entities (Brussels: Official Journal of the European Union, 2023).

[41] Dan Sandu and Mariam Bitsadze, *Securing the Black Sea: NATO, EU Integration, and the Struggle Against Russian Influence* (Tbilisi: Friedrich-Naumann-Foundation for Freedom South Caucasus, April 2025), 15-16.

[42] Sandu and Bitsadze, *Securing the Black Sea*, 16–17.

Infrastructure and transport corridors remain inadequate for rapid reinforcement, and alignment between NATO planning and EU connectivity projects, such as the Three Seas Initiative and the Trans-European Transport Network, has progressed unevenly.[43] Coordination across land, air and maritime domains also remains inconsistent: political and legal constraints, particularly the Montreux Convention, limit NATO's naval flexibility, while investment in integrated air and missile defence remains patchy. Initiatives such as the European Sky Shield mark progress, yet Black Sea states have not reached the interoperability standards of their northern Allies.[44]

Finally, cooperation with regional partners such as Ukraine, Georgia, and Moldova remains dispersed. Lancaster emphasizes that resilience-building efforts require "sustained coordination among Allies and institutions to avoid duplication and delay," but current initiatives are scattered across NATO programmes, EU mechanisms, and U.S. bilateral aid.[45] In practice, the region exemplifies a persistent coordination gap: despite shared strategic intent, transatlantic actors continue to diverge in execution, leaving hybrid deterrence in the Black Sea less coherent and less agile than in the Baltic.

4.3 Cross-Regional Coordination Gaps and Policy Recommendations

The Baltic and Black Sea case studies reveal a set of structural coordination gaps that transcend regional specificities and affect the transatlantic response to hybrid threats on land. In both theatres, low-intensity sabotage, cyber operations and pressure on critical infrastructure exploit persistent difficulties in attribution and threshold-setting, especially when incidents remain below the perceived level of an "armed attack".[46] This ambiguity interacts with overlapping mandates among NATO, the EU, and the United States, producing uncertainty over who should lead and with which instruments.

At the operational level, fragmented intelligence-sharing and the absence of fully integrated situational awareness systems prevent the timely detection of hybrid campaigns that link maritime incidents, cyber intrusions and land-based vulnerabilities in logistics hubs, energy grids and transport corridors.[47] Uneven investments in resilience and critical infrastructure protection further exacerbate these problems, creating weak points along the eastern flank that adversaries can target to generate disproportionate strategic effects.

Addressing these cross-regional gaps requires a shift from nationally framed, reactive responses towards a more anticipatory and integrated hybrid deterrence posture.[48] As a first step, this paper proposes that NATO, the EU and

[43] European Commission, *Military Mobility: An EU Action Plan (Military Mobility 2.0)*, COM(2022) 608 final (Brussels, 2022).
[44] NATO, *NATO Integrated Air and Missile Defence Policy* (Brussels, 2025).
[45] Sandu and Bitsadze, *Securing the Black Sea*, 17-18.
[46] Hanns Seidel Foundation, "Strategic Vulnerabilities: Hybrid Warfare Threats from Russia and China on Europe's Critical Infrastructures," August 26, 2025.
[47] Genini, Davide. "Countering Hybrid Threats: How NATO Must Adapt (Again) After the War in Ukraine." Critical Assessment: A Roadmap, SAGE Journals, 2025.
[48] NATO, *Strategic Concept 2022*, paras. 13–16, 26.

the United States establish a Transatlantic Hybrid Attribution Cell (THAC). This would be responsible for producing joint technical and political assessments of hybrid incidents. Such a mechanism has the potential to reduce ambiguity over responsibility, enable coordinated signalling and prevent adversaries from exploiting institutional divisions among Allies.[49]

Strategically, NATO, the EU and the United States should converge on clearer definitions and operational thresholds for hybrid attacks, underpinned by a shared taxonomy of indicators and an escalation ladder that links specific hybrid activities to possible collective responses short of full-scale military action.

This should be complemented by strengthened intelligence architectures: deeper support for the EU's Single Intelligence Analysis Capacity and Hybrid Fusion Cell, closer EU–NATO arrangements for exchanging sensitive information, and more systematic alignment between U.S. bilateral initiatives and multilateral frameworks.[50] Allowing both the EU Hybrid Toolbox and NATO support mechanisms to be activated on an ex ante basis, when credible warning signs emerge, would help move from a predominantly reactive towards a preventive approach.

From a land-security perspective, policy efforts should prioritise the protection and redundancy of cross-border corridors and critical infrastructure connecting the Baltic and Black Sea regions - rail, roads, energy nodes and logistics hubs - whose disruption would undermine broader transatlantic deterrence. More systematic alignment is needed between U.S. bilateral initiatives, NATO planning and EU regulatory frameworks, particularly in regions where mobility and reinforcement gaps remain substantial.[51]

Regular cross-regional exercises integrating civilian agencies, private-sector operators and Allied forces would help operationalise these mechanisms and strengthen coherent deterrence across the eastern flank. Ultimately, a joint EU–NATO–U.S. hybrid-crisis roadmap could codify roles, instruments and non-Article-5 responses, from sanctions to coordinated strategic communication, while ensuring that no single region, whether Baltic or Black Sea, becomes the weak link in the transatlantic land-security architecture.[52]

5. Conclusion

Hybrid threats have redefined the boundaries between peace and conflict, challenging the conceptual and operational foundations of Euro-Atlantic security. This paper has shown that NATO, the European Union and the

[49] Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracies," *International Affairs* 95, no. 2 (2019): 255–275.

[50] Lasoen, Kenneth. Realising the EU Hybrid Toolbox: Opportunities and Pitfalls. The Hague: Clingendael Institute, December 2022.

[51] Gaiser, Laris. "NATO - EU Collaboration on Hybrid Threats: Cooperation Out of Necessity with Potential Consequences on International Legal Framework." National Security and the Future 1–2 (20) (2019).

[52] Zandee, Dick; van der Meer, Sico; Stoetman, Adája. Countering Hybrid Threats: Steps for Improving EU–NATO Cooperation. The Hague: Clingendael Institute, October 2021.

United States have progressively aligned their approaches to hybrid warfare, converging around the principles of resilience, preparedness and cross-domain deterrence. Yet, as the Baltic and Black Sea cases illustrate, this convergence remains incomplete. While the Baltic region demonstrates how coordinated military presence, societal resilience and integrated intelligence mechanisms can generate an effective hybrid deterrence posture, the Black Sea reveals the limits of such coordination when institutional, political and logistical asymmetries persist.

The findings of this study point to a structural gap: transatlantic hybrid deterrence is strongest where institutional mandates, technical capabilities and political priorities interact seamlessly, and weakest where mismatches between NATO's defence orientation, the EU's regulatory instruments and U.S. bilateral frameworks remain unresolved. The persistence of fragmented intelligence-sharing, uneven infrastructure protection and ambiguous threshold-setting continues to provide adversaries with exploitable openings, particularly in regions marked by complex geopolitical constraints.

Strengthening hybrid deterrence therefore requires more than expanding military deployments or resilience initiatives. It demands a shift toward anticipatory and integrated crisis management: harmonised definitions of hybrid attacks, joint escalation pathways, interoperable situational awareness systems, and coordinated activation of NATO and EU hybrid response mechanisms. Ensuring the protection and redundancy of critical land corridors linking the Baltic and Black Sea regions is equally essential, as disruptions in these nodes could rapidly undermine collective defence.

Ultimately, the effectiveness of transatlantic hybrid deterrence will depend on whether NATO, the EU and the United States can operationalise the political alignment that now exists at the strategic level. A more coherent division of labour (military, civilian, economic and technological) offers the most credible path to denying adversaries the ability to exploit institutional seams. If successfully implemented, such an integrated approach would transform hybrid threats from a source of vulnerability into a catalyst for deeper transatlantic cohesion.

Bibliography

Atlantic Council. "The Pentagon's Focus on the Gray Zone." Scowcroft Center for Strategy and Security, Gray Zone Task Force, December 13, 2022.

Chatham House. Hybrid Warfare in Europe: Lessons from Ukraine. London: Chatham House, 2022.

CSIS (Center for Strategic and International Studies). Resilience in the Gray Zone. Washington, DC: CSIS, 2022.

European Centre of Excellence for Countering Hybrid Threats. Annual Report 2023. Helsinki: Hybrid CoE, 2023.

European Commission. Joint Framework on Countering Hybrid Threats: A European Union Response. Brussels: European Commission, 2016.

European Commission. The EU's Cybersecurity Strategy for the Digital Decade. December 16, 2020. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

European Commission. *Military Mobility: An EU Action Plan (Military Mobility 2.0).* COM(2022) 608 final. Brussels, 2022.

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. Joint Framework on Countering Hybrid Threats: A European Union Response. Brussels: European External Action Service, 2016.

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament and the Council: The European Union's Strategic Approach to the Black Sea Region. JOIN (2025) 135 final. Brussels, May 28, 2025.

European Council. EU–NATO Joint Declaration on Cooperation. Brussels, January 10, 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/.

European External Action Service (EEAS). EU Strategic Approach to the Black Sea Region. Last updated March 11, 2024. https://www.eeas.europa.eu/eeas/eu-strategic-approach-black-sea-region_en.

European Parliament. Background Note, Session I: Protection and Securing the European Union — Hybrid Threats as an External Factor Destabilising Europe. Brussels: European Parliament, March 19, 2024.

European Union. Directive (EU) 2023/1230 on the Resilience of Critical Entities. Brussels: Official Journal of the European Union, 2023.

European Union. Revised EU Maritime Security Strategy. Brussels: European External Action Service, 2023.

Gaiser, Laris. "NATO–EU Collaboration on Hybrid Threats: Cooperation Out of Necessity with Potential Consequences on International Legal Framework." National Security and the Future 1–2 (20) (2019).

Genini, Davide. "Countering Hybrid Threats: How NATO Must Adapt (Again) After the War in Ukraine." Critical Assessment: A Roadmap. SAGE Journals, 2025.

Giles, Keir. Russia's New Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. London: Chatham House, 2016.

Hanns Seidel Foundation. "Strategic Vulnerabilities: Hybrid Warfare Threats from Russia and China on Europe's Critical Infrastructures." August 26, 2025.

Hoffman, Frank G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.

Hybrid Centre of Excellence. Russia's Hybrid Threat Tactics against the Baltic Sea Region. Helsinki: Hybrid CoE, 2024.

Lasoen, Kenneth. Realising the EU Hybrid Toolbox: Opportunities and Pitfalls. The Hague: Clingendael Institute, December 2022.

Mazarr, Michael J. Mastering the Gray Zone: Understanding a Changing Era of Conflict. Carlisle Barracks, PA: U.S. Army War College Press, 2015.

Miętkiewicz, Rafał. "Hybrid Threats in the Baltic Sea: The Results of Analysis of Countermeasure Options." Scientific Journal of the Polish Naval Academy 234, no. 3 (2023): 58–61.

NATO. "Cyber Defence Overview." Last updated March 2023. https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO. "Hybrid Threats." NATO Official Portal. Last updated 2024. https://www.nato.int/cps/en/natohq/topics_156338.htm.

NATO. Hybrid Threats and Hybrid Warfare: Resilience in Practice. Brussels: NATO Strategic Communications Centre of Excellence, 2024.

NATO. *NATO Integrated Air and Missile Defence Policy*. Brussels, 2025.

NATO. "Strategic Concept." June 29, 2022. https://www.nato.int/strategic-concept.

NATO. "Strengthening NATO's Eastern Flank." Last updated October 23, 2025.

https://www.nato.int/cps/en/natohq/topics_136388.htm.

NATO. "Wales Summit Declaration." September 5, 2014. https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO. "Warsaw Summit Communiqué." July 9, 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO Parliamentary Assembly. Black Sea Security Report. Brussels: NATO PA, 2023.

Pynnöniemi, Katri, and András Rácz. Russia's Hybrid Warfare: A New Challenge for Europe and the Atlantic Alliance. FIIA Report 45. Helsinki: Finnish Institute of International Affairs, 2016.

Renz, Bettina. Russia's Military Revival. Cambridge: Polity Press, 2018.

Sandu, Dan, and Mariam Bitsadze. Securing the Black Sea: NATO, EU Integration, and the Struggle Against Russian Influence. Tbilisi: Friedrich-Naumann-Foundation for Freedom South Caucasus, April 2025.

U.S. Department of Defense. National Defense Strategy of the United States of America: 2022. Washington, DC: U.S. Government Publishing Office, 2022.

U.S. Department of Defense. National Defense Strategy of the United States of America 2022, including the Nuclear Posture Review and Missile Defense Review. Washington, DC: Department of Defense, 2022.

U.S. Department of State. Strategy for Security in the Black Sea Region. Washington, DC: U.S. Government Printing Office, 2023.

U.S. European Command. Statement of Gen. Christopher G. Cavoli to the House Armed Services Committee, April 26, 2023.

https://www.eucom.mil/document/42351/gen-christopher-g-cavoli-2023-posture-statement-to-the-hasc.

Zandee, Dick, Sico van der Meer, and Adája Stoetman. Countering Hybrid Threats: Steps for Improving EU–NATO Cooperation. The Hague: Clingendael Institute, October 2021.