SECURING THE FRONTLINES:

Experimentalist Governance for Critical Maritime Infrastructure in the Black Sea and North Sea

AUTHORS:

Dr. Jakub Godzimirski, Research Professor,
Norwegian Institute of International Affairs

Sergiu Mitrescu, Program Director,
New Strategy Center

NEW STRATEGY CENTER

NUPI Norwegian Institute of International Affairs

Dr. Jakub GODZIMIRSKI is a Research Professor at NUPI. He has been working on Russian foreign and security policy issues for more than 20 years, paying special attention to the role of energy resources in Russian grand strategy. In addition, he also has worked on European policy and its impact on developments in Central and Eastern Europe, including relations with Russia.

Sergiu MITRESCU is the Program Director of New Strategy Center and a senior expert on hybrid threats and maritime security, with a particular focus on critical maritime infrastructure. His work centres around the intersection of hybrid threats and maritime security, focusing on Black Sea dynamics.

Editor: **George SCUTARU**, Chief Executive Officer, New Strategy Center, Former National Security Advisor to the President of Romania

The development of this policy paper benefited from the careful documentation work carried out during its preparation, with particular support from Dilara Kalliloglu, Ion Cristea and Răzvan Ceuca, whose contributions proved essential at key stages of the research process.

The study is published under the Strategic Initiative for Defending Critical Maritime Infrastructure (SIDMI) project financed through the Romania Norway Bilateral Fund 2014-2021, financing contract 17369/26.04.2024.

Disclaimer: This text contains the personal opinions and perspective of the authors and does not necessarily reflect the views of the New Strategy Center or the Norwegian Institute of International Affairs

Cover Photo: @starline, Freepik

Iceland
Liechtenstein
Norway grants

Securing the Frontlines: Experimentalist Governance for Critical Maritime Infrastructure in the Black Sea and North Sea

1. Introduction

The proliferation of hybrid threats challenges both national security and the institutional foundations of governance. Nowhere is this tension more acute than in the maritime domain, where critical infrastructure such as undersea cables, offshore energy platforms, and subsea pipelines have become both economic lifelines and geopolitical fault lines. These infrastructures are increasingly exposed to hybrid operations designed to exploit legal ambiguity, attribution challenges, and the seams between civil, military, and private actors.

Traditional security governance models premised on clear jurisdictional boundaries, centralized command structures, and rigid doctrinal templates, struggle to account for weaponized ambiguity and threats operating below thresholds of open conflicts. As sub-threshold threats continue to evolve and be refined, they reveal deep structural limitations in existing institutional responses, including sectoral silos, information-sharing deficits, and accountability systems ill-suited for dynamic crisis environments.

This paper explores the need for more adaptive governance frameworks capable of managing the uncertainty, complexity, and cross-sectoral interdependence that define today's hybrid threat landscape. Specifically, it examines how Experimentalist Governance (EG), a recursive, peer-informed model of problem-solving, offers a promising architecture for coordinating the defense of critical maritime infrastructure (CMI) in the face of hybrid aggression.

The paper analyzes two distinct cases: Norway, with its mature institutional capacity, dense subsea infrastructure, and strong integration with NATO and EU partners; and Romania, situated at the Black Sea frontier, where emerging offshore energy projects intersect with a fluid and contested security environment. While these cases differ in institutional maturity and strategic context, both demonstrate how EG principles, provisional goal-setting, local discretion, peer review, and iterative learning, can serve as practical tools for strengthening CMI resilience under hybrid pressure.

This paper seeks to move beyond conventional threat analysis to offer operational recommendations for policy design, governance innovation, and cross-sectoral coordination, recognizing that the hybrid challenge is not only technical or legal, but fundamentally institutional. In doing so, it builds on previous joint research by the authors, which mapped the evolving spectrum of hybrid threats and strategic pressures targeting critical maritime infrastructure in the Black Sea and North Sea regions, with particular attention to Russian Next-Generation Warfare, cyber vulnerabilities, and emerging dual-use infrastructure risks.

2. Experimentalist governance

2.1 The Limits of Traditional Governance in Hybrid Threat Environment

The Governance Gap

The responses of states and actors contending with the continuum of conflict created by the proliferation of hybrid threats permeates the institutional logic of governance itself. Traditional governance systems, built for a world of stable actors, clear lines of authority, and predictable escalation pathways, struggle to keep pace. The very features that once made hierarchical institutions effective, centralized control, rule-based procedures, and rigid accountability chains, now act as liabilities when confronting adversaries who operate below the threshold of open conflict, and who weaponize ambiguity to delay or complicate response. As Bueger and Edmunds[1] observe, the ocean is no longer a stage for routine governance but has become a contested domain where strategic instability and infrastructural fragility intersect. Hybrid attacks on critical maritime infrastructure (CMI) test more than detection systems or defensive capacity, they test the governance resilience of institutions tasked with protecting it. As will be shown, this governance gap is not incidental; it is systemic, and it demands an institutional response that is both reflexive and adaptive.

The Failure of Command-and-Control in Hybrid Environments

At the heart of this institutional tension is the command-and-control logic that underpins most national crisis governance models. These models assume a linear progression from detection

[1]Bueger, C. and Edmunds, T. (2017). Beyond seablindness: a new agenda for maritime security studies. International Affairs, 93(6), pp. 1293–1311. Available at: https://doi.org/10.1093/ia/iix174

to decision-making, governed by vertical authority structures, scripted response protocols, and legal clarity. However, hybrid threats are non-linear by design. They are meant to disrupt, confuse, and delay, often unfolding through a sequence of deniable actions that cut across bureaucratic boundaries and jurisdictional domains. Such threats resemble transboundary crises: events that transcend sectoral borders, overwhelm existing procedures, and generate uncertainty about both causes and consequences. In such contexts, hierarchies produce reactive responses not due to a lack of capacity, but due to a lack of adaptability.[2]

This dilemma is exemplified by Sweden's recalibration of its national security posture. The country's shift from globalized risk management to a state-centric total defence model sought to clarify institutional roles and reinforce preparedness. Yet as Berndtsson[3] shows, in practice,it generated doctrinal tensions: uncertainty about thresholds for action, confusion over which agency should respond to hybrid intrusions, and a lack of clarity on the legal framing of cyber-physical disruptions. Sweden's experience reflects a broader pattern, where hybrid events fall into procedural gray zones, often too ambiguous to be escalated, yet too disruptive to avoid arising a response.

The Problem of Siloed Institutions and Reactive Learning

A key barrier to effective hybrid threat response lies in the institutional fragmentation that characterizes most national and regional governance architectures. Maritime infrastructure protection involves a range of actors, including navies, coast guards, regulatory agencies, intelligence services, port authorities, and private operators, yet few mechanisms exist to synchronize their actions in real time, especially under ambiguous conditions. The result is a governance system that is reactive, rather than anticipatory.

In the Norwegian case, early failures in responding to complex maritime incidents were not primarily due to capacity gaps, but to information-sharing deficits and unclear coordination protocols.[4] These issues were eventually addressed through the creation of more integrated

---

[2] Boin, A., Ekengren, M. and Rhinard, M. (2013). The European Union as Crisis Manager: Patterns and Prospects. Cambridge University Press.

[3] Berndtsson, J. (2025). *Hybrid Threats and the "New" Total Defence: The Case of Sweden*. In: Borch, O.J. and Heier, T. (eds.) *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response*. Routledge

[4] Sandbakken, C. and Karlsson, R. (2025). *Information Sharing in Complex Crises: Experiences from the Norwegian Maritime Sector*. In: Borch, O.J. and Heier, T. (eds.) *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response*. Routledge.

maritime situational awareness centers, but only after repeated stress events exposed institutional blind spots. In this sense, Norway's progress was driven less by doctrinal foresight than by institutional self-correction.

This finding is echoed in broader governance literature. Ansell and Gash[5] argue that collaborative governance only functions effectively when supported by shared platforms for mutual learning, joint goal-setting, and iterative feedback. Yet such platforms are often absent in traditional bureaucratic systems, which operate on the basis of discrete mandates and sectoral silos. This leads to predictable frictions: maritime response delays caused by confusion over jurisdiction, or private cable operators being excluded from early-warning systems, despite being the first to detect disruptions.

The absence of horizontal integration mechanisms not only hinders operational response but also undermines the ability to recognize hybrid threat patterns, which often manifest as subtle anomalies across multiple domains. Without a framework for pooling weak signals across agencies and sectors, the strategic intent behind hybrid actions and their cascading effect is often missed.

Rigid Accountability and Inflexible Doctrine

Another structural shortcoming of traditional governance in the hybrid domain lies in its accountability logic. Most institutional accountability systems are designed to assign blame post hoc, rather than enable rapid, adaptive decision-making in conditions of uncertainty. This results in governance cultures that prioritize compliance with procedure over performance under pressure. Ebrahim[6] calls this dynamic "accountability myopia", a condition where adherence to rules and protocols overshadows the need for organizational learning. In a hybrid threat context, where actions unfold across multiple sectors and domains with ambiguous attribution, rigid accountability models tend to paralyze response mechanisms. Decision-makers fear overstepping their mandates, and cross-sectoral improvisation is discouraged in favor of risk-averse (in)action.

This rigidity is especially dangerous in tightly coupled, high-risk systems, such as undersea energy grids, maritime chokepoints, and data cable networks. Charles Perrow's theory of

---

[5]Ansell, C. and Gash, A. (2008). Collaborative Governance in Theory and Practice. Journal of Public Administration Research and Theory, 18(4), pp. 543–571. Available at: https://doi.org/10.1093/jopart/mum032

[6]Ebrahim, A. (2005). Accountability Myopia: Losing Sight of Organizational Learning. Nonprofit and Voluntary Sector Quarterly, 34(1), pp. 56–87.

"normal accidents"[7] emphasizes that in such systems, small failures can rapidly cascade if institutions are incapable of adaptive response. Hybrid threats exploit precisely this vulnerability by introducing low-level stressors that gradually degrade systemic coherence. Moreover, post-incident inquiries, while essential for democratic accountability, often fail to generate forward-looking reform if their findings are not embedded into iterative governance cycles. Too often, lessons from hybrid incidents are documented, but not internalized. Without institutional mechanisms to revise doctrine, update SOPs, and restructure response hierarchies, accountability becomes a backward-looking ritual rather than a tool for building resilience.

Governance Under Pressure

Hybrid threats reveal the brittle edges of traditional security governance. Institutional hierarchies are often too slow to respond in real time, with sectoral silos creating blind spots in detection and attribution. Accountability systems remain backward-looking, focused more on assigning blame than fostering anticipatory adaptation. These structural limitations are not incidental, they are systematically reproduced in governance systems designed for linear escalation and clear jurisdictional boundaries. In the fluid, contested spaces of maritime hybrid threats, such systems cannot deliver the agility, cross-sectoral learning, or iterative refinement that crisis response demands. This cumulative breakdown underscores the need for a recursive, learning-oriented, and peer-informed governance model, one that embraces experimentation, rewards transparency, and builds institutional capacity through deliberate feedback mechanisms. Experimentalist Governance (EG) offers such a model. The next section introduces its architecture and explains why it is uniquely suited to managing complexity under uncertainty.

2.2. What Is Experimentalist Governance?

Experimentalist governance (EG) is a form of adaptive, deliberative governance designed to operate under conditions of uncertainty, complexity, and institutional fragmentation. As

[7] Perrow, C. (1994). Normal Accidents: Living with High-Risk Technologies. Princeton University Press.

developed by Sabel and Zeitlin,[8] EG emerged in response to the growing recognition that traditional, rule-based and hierarchical governance frameworks were insufficient for managing policy domains where no single actor possesses full authority, information, or capacity.

At its core, EG is a recursive problem-solving architecture, composed of four interlinked steps:

1. Provisional Goal-Setting: Rather than establishing rigid rules from the outset, EG begins with the joint definition of framework goals and performance indicators. These are typically broad enough to accommodate national and local diversity, yet concrete enough to permit comparative assessment.

2. Local Adaptation and Experimentation: Decentralized units—whether national agencies, subnational authorities, or public-private partnerships, are granted autonomy to implement the goals as they see fit, taking into account their specific circumstances and capacities. This discretion fosters innovation, responsiveness, and contextual relevance.

3. Peer Review and Monitoring: Units are required to regularly report on their performance, which is then subjected to horizontal review and benchmarking. This creates transparency, allows mutual learning, and reduces the risk of institutional complacency or free-riding.

4. Iterative Revision of Framework Goals: The framework itself is periodically revised based on implementation feedback, emerging knowledge, and lessons learned across contexts. This built-in loop of revision is what makes EG a living governance system rather than a static policy regime.

This architecture has been widely applied within the European Union in domains such as environmental regulation, competition policy, data protection, and cross-border infrastructure development. In each of these areas, EG has enabled cooperation among diverse actors, often with divergent legal traditions, capabilities, and political priorities, by promoting flexibility, learning, and deliberation instead of rigid compliance.

---

[8] Sabel, C.F. and Zeitlin, J. (2010). Experimentalist Governance in the European Union: Towards a New Architecture. Oxford University Press; Sabel, C.F. and Zeitlin, J. (2012). Experimentalist Governance. In: Levi-Faur, D. (ed.) The Oxford Handbook of Governance, Oxford University Press, pp. 169–183.

Importantly, EG is not anti-institutional or anarchic. It is highly structured, but that structure is dynamic and reflexive, designed to coordinate complexity without flattening difference. It substitutes traditional command-and-control with peer accountability, adaptive coordination, and recursive goal adjustment. This model holds particular promise for managing hybrid threats to critical maritime infrastructure, where ambiguity, distributed responsibility, and the need for rapid adaptation challenge the effectiveness of centralized, rules-based approaches. The following section explores how the principles of EG, local discretion, peer learning, and recursive planning, map onto the unique operational and strategic demands of protecting CMI in a hybrid threat environment.

2.3. Why Experimentalist Governance Is Well-Suited to Hybrid Threats and CMI Protection

The protection of critical maritime infrastructure (CMI) in the face of hybrid threats requires a governance model capable of functioning under strategic ambiguity, jurisdictional fragmentation, and rapidly evolving risk vectors. Traditional security governance models struggle in such contexts because they are structured around predictability, vertical authority, and stable mandates, none of which characterize hybrid threat environments. Experimentalist governance (EG), by contrast, is expressly designed for coordination under uncertainty, making it a particularly fitting framework for addressing the multifaceted challenges posed by hybrid campaigns.

Hybrid threats operate by design below the threshold of war, across civil-military boundaries, and in ways that intentionally obscure attribution. Such tactics demand dynamic situational awareness, multi-sectoral coordination, and institutional reflexivity. EG offers this by structuring collaboration around provisional goal-setting, local discretion, peer review, and iterative revision, a model that supports adaptation, feedback, and decentralised problem-solving. Consider the challenge of setting thresholds for response to incidents like GPS spoofing near offshore infrastructure or the probing of undersea cables by unmarked vessels. Traditional frameworks often falter in determining whether such incidents fall under military jurisdiction, law enforcement, or regulatory response. EG allows actors to set interim benchmarks collaboratively, test them in practice, and adjust them based on collective review, without waiting for legal certainty or centralized authorization. This flexibility is crucial in hybrid environments where ambiguity is weaponized.

Moreover, EG's emphasis on peer learning and transparency addresses the chronic fragmentation between sectors and agencies that undermines hybrid threat response. For instance, as seen in Norway's development of joint maritime information-sharing centers,[9] performance improved not through rigid command alignment, but through iterative coordination between civilian, military, and commercial actors. These initiatives reflect core EG features: multi-actor experimentation, shared performance metrics, and feedback loops that inform doctrinal updates. Another advantage of EG in this context is its capacity to generate learning across heterogeneous institutional settings. For example, while Norway and Romania differ in institutional maturity, geographic exposure, and alliance integration, both face similar hybrid risks. EG does not require full harmonization between these states; rather, it supports structured diversity, allowing each actor to adapt while still participating in shared review and iterative improvement. This is particularly valuable in EU and NATO settings, where a single prescriptive doctrine would be either too rigid or politically unworkable. Finally, EG aligns with the need for cyber-legal-operational integration, as highlighted in proposals for hybrid threat triage protocols.[10] Instead of static playbooks, EG supports governance regimes in which SOPs evolve, attribution methods are refined through use, and public-private coordination mechanisms are constantly adjusted in response to threat evolution.

In sum, experimentalist governance offers a realistic, flexible, and politically feasible alternative to traditional security governance models. Its recursive structure and deliberative logic make it not only compatible with the hybrid threat environment, but potentially transformative, able to shift the institutional mindset from control and containment to adaptive learning and resilience-building across the CMI protection ecosystem.

While Experimentalist Governance offers significant advantages for managing hybrid threats under conditions of uncertainty, its implementation is not without obstacles. Successful EG requires high levels of trust among participating actors, willingness to share sensitive information, and sustained political commitment to iterative adaptation, all of which can be difficult to achieve in fragmented or contested regional environments. In the Black Sea context, historical tensions, sovereignty sensitivities, and diverging national threat perceptions may complicate efforts to establish transparent peer review and shared learning mechanisms. Similarly, in mature systems like Norway, bureaucratic inertia and sectoral path dependencies

---

[9] Sandbakken and Karlsson (2025), *Information Sharing in Complex Crises.*

[10]Mazaraki, N. and Goncharova, Y. (2022). Cyber Dimension of Hybrid Wars: Escaping a 'Grey Zone' of International Law to Address Economic Damages. Baltic Journal of Economic Studies, 8(2), pp. 115–120.

may limit the scope for institutional experimentation. Recognizing these barriers is essential to designing EG frameworks that are both politically feasible and operationally resilient.

3. Strategic Responses to the Hybrid Challenge to CMI

The maritime domain exemplifies what Kilcullen[11] describes as liminal warfare, a form of conflict that unfolds in ambiguous, in-between spaces where traditional legal, military, and political responses become uncertain. In this gray zone, hybrid actors exploit legal seams, attribution difficulties, and operational ambiguity to probe infrastructure, assert strategic presence, and undermine resilience, all while avoiding overt acts that would trigger a conventional response. Tactics such as AIS spoofing, cable tapping, or dark vessel anchoring are not random anomalies. Rather, they are deliberate instruments of liminal pressure, calibrated to advance strategic objectives without crossing formal thresholds of war, while blending with recurrent accidents and practices which further augment their plausible deniability.

Borch and Heier[12] describe these hybrid actions as part of an iterative, adaptive campaign to test red lines and gradually normalize aggressive behavior. The repeated presence of dark vessels with inactive AIS, seabed intrusions disguised as environmental surveys, and disinformation targeting navigational systems all fall into this pattern of “gray zone” warfare. These actions blur the boundary between civil and military, peace and conflict, lawful and coercive. Defending critical maritime infrastructure (CMI) under these conditions requires more than just surveillance, it demands pre-scripted escalation thresholds, real-time situational awareness, and doctrinal clarity on what type of action warrants civilian, legal, or military response.

Within this landscape, strategic planning must be both dynamic and iterative, accounting for shifting political sensitivity, ambiguity about intent, and the ever-present risk of misattribution and inadvertent escalation.[13] Their model highlights the need to bridge civilian and military planning logics while operating under intersectoral resource constraints. Because hybrid

---

[11]Kilcullen, D. (2020). The Dragons and the Snakes: How the Rest Learned to Fight the West. Oxford University Press.

[12] Borch, O.J. and Heier, T. (2025). *Toward a Hybrid Threat Response Model*. In: Borch, O.J. and Heier, T. (eds.) *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response*. Routledge.

[13] ibid.

threats thrive in systems of mutual dependency and interconnected vulnerabilities, especially in sectors like energy and maritime infrastructure, strategic planning must link with operational agility and knowledge development in a continuous feedback loop.

Finally, hybrid attacks on CMI must be interpreted not just as technical intrusions, but as strategic signals.[14] A cyber disruption to a platform, a vessel anomaly, or a satellite blackout may appear isolated on a technical dashboard, but geopolitically, these are often part of a broader signaling campaign. Recognizing this interpretive dimension is essential: situational awareness is not only about detection, but about understanding intent. This interpretive layer serves as the bridge to attribution and deterrence, which will be explored in the next subsection.

Deterrence Under Ambiguity: Rethinking Maritime Signaling

Hybrid threats operate deliberately below the thresholds of detection, attribution, and retaliation, exploiting ambiguity to erode strategic stability without crossing into open conflict.[15] This strategic use of deniability undermines conventional deterrence models by avoiding the triggers that would prompt defensive responses. In such an environment, maritime deterrence must adapt not only in its tools, but in its logic, rethinking how presence, posture, and signaling operate in legally and politically ambiguous settings.

Recent experimental findings by Pischedda and Cheon[16] reinforce this point: their study focused on the war in Ukraine demonstrated that unattributed attacks do not increase the likelihood of concessions from the target population. In fact, they may produce a backlash effect, generating stronger public resistance, especially when the attack is perceived as deliberately unclaimed to avoid accountability. Even when attribution is uncertain, threat perception remains high, and the will to resist is undiminished. These findings challenge the strategic value of plausible deniability and suggest that, in some cases, transparency may be a more effective coercive or deterrent tool than covert action.

---

[14] Irshad, E. and Siddiqui, A.B. (2024). *Context-Aware Cyber-Threat Attribution Based on Hybrid Features*. ICT Express, 10(3), pp. 553–569. Available at: https://doi.org/10.1016/j.icte.2024.04.005

[15] Balcaen, P., Du Bois, C. and Buts, C. (2021). *A Game-Theoretic Analysis of Hybrid Threats*. Defence and Peace Economics, 33(1), pp. 26–41. Available at: https://doi.org/10.1080/10242694.2021.1875289

[16] Pischedda, C. and Cheon, A. (2023). *Does Plausible Deniability Work? Assessing the Effectiveness of Unclaimed Coercive Acts in the Ukraine War*. Contemporary Security Policy, 44(3), pp. 345–371.

This has direct implications for maritime deterrence. Naval forces are often framed as reactive or supportive, not decisive, a conceptual legacy that constrains their role in strategic signaling. Yet in the hybrid domain, persistent, credible maritime posture is precisely what enables states to deny deniability.[17] A visible, rules-based naval presence, anchored in ISR coverage and narrative framing, can deter sub-threshold action not by threatening retaliation, but by preempting ambiguity.

Balcaen et al.[18]offer a valuable framework for understanding this recalibration of deterrence. They propose three analytical thresholds, detection, attribution, and retaliation, which provide a lens through which maritime deterrence can be assessed. These thresholds help identify where vulnerabilities lie: in ISR blind spots, attribution delays, or doctrinal ambiguity about what constitutes a trigger for escalation. Using these thresholds, this paper advocates a shift in emphasis, from punitive deterrence to deterrence by resilience and visibility, where surveillance, attribution readiness, and institutional clarity are prioritized. Moreover, strategic deterrence must be cost-sensitive. Their game-theoretic model[19] suggests that investing heavily in high-end naval assets may not yield optimal results when defending long, diffuse maritime infrastructure. Instead, more effective returns may come from layered investments in situational awareness, cross-sector coordination, and legal preparedness, especially when combined with posture designed to deny deniability and shape perceptions before escalation occurs.

In sum, the challenge is not a lack of capability, but a lack of conceptual readiness. Deterrence in the hybrid maritime domain is constrained by the way naval forces are imagined, not by their actual utility.[20] To be effective, maritime deterrence must be understood not just in terms of ships or firepower, but in terms of presence, visibility, and the clarity of the signals being sent in a strategically ambiguous environment.

---

[17] Björnehed, E. (2022). *What Is the Value of Naval Forces? – Ideas as a Strategic and Tactical Restriction*. Defence Studies, 22(1), pp. 1–15. Available at: https://doi.org/10.1080/14702436.2021.1931133

[18] Balcaen et al. (2021). *A Game-Theoretic Analysis of Hybrid Threats*.

[19] ibid.

[20] Björnehed (2022). *What Is the Value of Naval Forces?*

Attribution as a Strategic Challenge and Leverage

In the hybrid threat environment, attribution is both technically challenging and politically sensitive. For example, traditional cyber forensics rely heavily on technical signatures, such as IP addresses, malware code, or known tactics, these indicators are increasingly easy to obfuscate, spoof, or misdirect[21]. As a result, the threshold for establishing credible attribution, especially in the maritime domain, is continually rising, just as adversaries grow more comfortable operating within the space between disruption and deniability. As Nilsson, Weissmann & Palmertz[22] argue, "warning intelligence processes aimed at protecting critical vulnerabilities across society must be rebalanced to detect synchronized, multi-vector hybrid attacks intentionally designed to fall outside and/or below traditional detection thresholds." Attribution, in this context, goes beyond technical accuracy; it is a political act with escalation, signaling, and legal consequences. States must therefore develop attribution systems that are both technologically robust and strategically aligned, with the end goal of facilitating the diplomatic-political decision to attribute such a malign action, an attribution which brings consequences of its own.

A key element in transforming attribution into deterrence lies in strategic communication. The case of pre-invasion intelligence disclosure in the lead-up to Russia's 2022 assault on Ukraine demonstrates how timely, calibrated public disclosure of classified findings can shift strategic narratives and shape adversary behavior. Pre-disclosure may deter covert occupation or sabotage by forcing aggressors to factor reputational risk into their cost calculus.[23] In the maritime context, this logic supports the need for maritime-specific attribution doctrines that allow for proactive, not reactive, signaling, especially when defending subsea infrastructure or responding to dark vessel incidents.

The complexity of attribution can also be understood through the detection, attribution, and retaliation framework mentioned above.[24] These thresholds can be used to assess the performance of ISR systems, the clarity of escalation pathways, and the political utility of attribution itself. In a hybrid environment, deterrence depends not only on the ability to strike

---

[21] Irshad and Siddiqui (2024). *Context-Aware Cyber-Threat Attribution*.

[22] Nilsson, N., Weissmann, M. and Palmertz, B. (2025). Hybrid Threats and the Intelligence Community: Priming for a Volatile Age. International Journal of Intelligence and CounterIntelligence, pp. 1–23. Available at: https://doi.org/10.1080/08850607.2024.2435265

[23] Ibid.

[24] Balcaen et al. (2021). *A Game-Theoretic Analysis of Hybrid Threats*.

back, but on the ability to attribute clearly and credibly, particularly in forums where legal, diplomatic, and reputational outcomes are shaped.

Ultimately, attribution is a strategic lever. It connects technology, intelligence, law, and communication. When executed deliberately, through interoperable systems, probabilistic attribution models, and pre-planned disclosure strategies, it can become a tool for compelling an adversary to change course before a crisis escalates, rather than a post-incident exercise in explanation.

3.1 EU

The EU defines critical infrastructure as 'a system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions' [25]. Critical infrastructure in the EU context is important not only because it ensures the functioning of the internal market but also because it is increasingly viewed as an important issue on the EU security and defence agenda that aims to strengthen the EU resilience.

The importance of these security and infrastructure related questions is increasingly recognized by the EU. In its White Paper on Defence published on 19 March 2025[26] the EU identified four priority multi-modal corridors (rail, road, sea and air) for military mobility for short-notice and large-scale movements of troops and equipment that the armed forces need access to. These four elements are fit for a dual-use and are to play a crucial part in a crisis situation with which both the EU and NATO will have to deal with when necessary.

In May 2025 the European Commission launched *The European Union's Strategic Approach to the Black Sea Region*,[27] a document that further underscores the growing institutional emphasis on protecting critical maritime infrastructure (CMI) within the hybrid threat landscape. The strategy explicitly identifies submarine cables, offshore energy platforms, gas and wind

---

[25] European Commission (2008). Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Available at: https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng

[26] European Commission (2025). Joint White Paper for European Defence Readiness 2030. European Commission. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/white-paper-future-european-defence-rearming-europe_en

[27] European Commission and High Representative (2025). *The European Union's Strategic Approach to the Black Sea Region*. JOIN(2025) 135 final, Brussels, 28 May 2025.

energy operations, and related maritime capabilities as priority assets for enhanced monitoring and protection, including through the establishment of a dedicated Black Sea Maritime Security Hub. Moreover, the strategy links CMI protection to broader hybrid threat mitigation, energy resilience, and EU-NATO coordination mechanisms, reinforcing the need for flexible, cross-sectoral governance models consistent with the experimentalist governance approach developed in this study.

3.2 NATO

NATO defines critical infrastructure as 'a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political and/or social life on which a nation and/or NATO depends'.[28] From the point of view of NATO critical infrastructure is important because it enables the fulfilment of its core tasks of deterrence and defence, crisis prevention and management and cooperative security. Security of energy supply has become one of the core interests of NATO since the Riga Summit in 2006 and Norway plays a key part as an energy supplier to Europe. Protection of the critical maritime infrastructure that plays an important role in this context has therefore become an important element on the alliance's agenda. NATO has developed a growing institutional ecosystem focused on the security of critical maritime infrastructure, including the newly established Maritime Centre for the Security of Critical Undersea Infrastructure in Northwood, UK, alongside specialized centers such as the NATO Centre for Maritime Research and Experimentation (CMRE), the Centre of Excellence for Maritime Security, and the Centre of Excellence for Operations in Confined and Shallow Waters.

3.3 Combined EU-NATO logic

Russian aggression against Ukraine and Russia's attacks on elements of critical infrastructure during this conflict as well as a growing realisation that elements of critical infrastructure are exposed to various types of Russian active measures and could be exposed to Russian kinetic attacks in the case of escalation of the conflict have made both the EU and NATO understand

[28]NATO (2019). Infrastructure Assessment. ACO Directive 084-002, 17 October 2019; Evans, C.V. (2022). Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency. NATO COE-DAT Handbook 1. US Army War College Press. Available at: https://press.armywarcollege.edu/monographs/955/

that there is a need for a closer cooperation between them to address various types of infrastructure-related challenges.

The EU and NATO have been working closely to enhance the resilience of critical infrastructure, especially in light of increasing security threats. Here are some key elements of their cooperation:

1. Resilience in Key Sectors: The cooperation focuses on critical sectors such as energy, transport, digital infrastructure, and space. These sectors are vital for both civilian and military operations

2. Information Sharing: Enhanced information exchange between the EU and NATO is crucial. This includes sharing threat intelligence and best practices to better anticipate and mitigate risks

3. Alternate Transport Routes: Identifying and securing alternate transport routes for both civilian and military mobility is a priority. This ensures that essential services and military operations can continue even if primary routes are disrupted

4. Security Research: There is a strong emphasis on collaborative security research to develop new technologies and strategies for protecting critical infrastructure

5. Hybrid Threats: Addressing hybrid threats, which combine physical and cyber-attacks, is a significant part of their cooperation. This is particularly relevant given the recent geopolitical tensions and conflicts

6. Structured Dialogue on Resilience: The EU-NATO Structured Dialogue on Resilience ensures coherent follow-up actions and political guidance to strengthen infrastructure resilience

These efforts are part of a broader strategy to ensure that critical infrastructure remains robust against evolving threats, thereby safeguarding essential services and economic stability.

The launching of the EU-NATO Task Force on resilience of critical infrastructure took place on 16 March 2023 and has opened a new era of cooperation between these two key organisations.[29] In June 2023 EU-NATO Task Force on the Resilience of Critical Infrastructure presented its Final Assessment Report[30] in which four sectors – energy, transport, digital infrastructure and space – were identified as critically important in the current context.

The key tasks of the the EU-NATO Task Force are:

- Mapping Security Challenges: The Task Force focuses on identifying and mapping out current security challenges that can affect critical infrastructure. This includes assessing vulnerabilities and potential threats in sectors such as energy, transport, digital infrastructure, and space.
- Recommendations for Cooperation: It provides concrete recommendations to deepen EU-NATO cooperation. This includes enhancing information exchanges, identifying alternate transport routes for civilian and military mobility, and fostering closer ties in security research.
- Parallel and Coordinated Assessments: The Task Force conducts parallel and coordinated assessments to ensure that both organizations are aligned in their efforts to mitigate potential vulnerabilities and enhance resilience.
- Political Guidance and Follow-Up: The Task Force ensures that the follow-up actions are coherent and aligned with the political guidance from both the EU and NATO. This structured approach helps in implementing the recommendations effectively.
- Sectoral and Cross-Sectoral Considerations: The Task Force addresses both sector-specific and cross-sectoral considerations to ensure a comprehensive approach to resilience. This helps in understanding the interdependencies between different sectors and mitigating cascading effects of disruptions.

---

[29] NATO, NATO and European Union launch task force on resilience of critical infrastructure, NATO, 2023 at https://www.nato.int/cps/en/natohq/news_212874.htm For more on the context see https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564.

[30]European Commission (2023). EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report. European Commission. Available at: https://commission.europa.eu/document/download/34209534-3c59-4b01-b4f0-b2c6ee2df736_en?filename=EU-NATO_Final%20Assessment%20Report%20Digital.pdf

Because Norway is a full-fledged member of NATO and has developed close cooperation with the EU through the EEA framework, the close cooperation between the EU and NATO on protection of critical infrastructure will also have positive effects on questions related to protection of the Norwegian critical maritime infrastructure. The same can be said about Romania that is a full-fledged member of both the EU and NATO and aims to become one of the important suppliers of energy to other members of these two organisations after having developed its maritime energy resources.

4. Operational Responses: The Case of Romania and Norway

4.1 Romania

Romania's growing role in the hybrid threat environment stems from both its strategic geography and its evolving critical maritime infrastructure (CMI) landscape. As a full member of both the European Union and NATO, Romania operates at the intersection of two major governance architectures, allowing it to leverage resources, norms, and institutional partnerships from both. However, unlike more mature infrastructure environments such as Northern Europe, Romania's maritime infrastructure remains at a relatively early stage of development, creating both vulnerabilities and opportunities for proactive governance innovation.

Compared to Northern Europe, Romania faces distinct regional challenges, including the war in Ukraine, persistent Russian hybrid operations, dark vessel activity, and complex jurisdictional overlaps in the Black Sea. These conditions exacerbate strategic ambiguity, legal uncertainty, and attribution difficulties. At the same time, they create a compelling case for adopting EG models, which emphasize iterative learning, peer-review mechanisms, and voluntary cross-border coordination even in the absence of fully harmonized legal frameworks.

While Romania already engages in cooperation with regional partners through the trilateral mine counter-measure coalition together with Bulgaria and Türkiye, which is expected to be expanded to cover the protection of CMI. EG offers a framework to coordinate such activities more systematically, allowing Romania, Bulgaria, Türkiye, and Ukraine to develop scalable protocols for data-sharing, joint incident reporting, legal interoperability, and cross-sector resilience benchmarking.

In this wider regional context, Türkiye's will continue to play a central role. Beyond its involvement in the trilateral mine counter-measure coalition, Ankara is actively supporting the Ukrainian Navy's modernization by constructing two corvettes tailored for Ukraine's needs. These vessels have recently undergone live-fire testing in the relative safety of the Sea of Marmara,[31]. While the corvettes are unlikely to be deployed before a settlement is reached, their construction in Türkiye reflects Ankara's strategic calculus: providing long-term naval support to Ukraine without provoking immediate escalation, while reinforcing its role as an anchor in any future Black Sea governance initiatives.

Importantly, Romania's hybrid threat governance posture is not developing in isolation. The EU-NATO Task Force on the Resilience of Critical Infrastructure aligns directly with Romania's emerging maritime infrastructure priorities. Romania's full participation in both organizations positions it uniquely to serve as a regional laboratory for institutional experimentation under real-time hybrid threat conditions.

In the immediate future, Romania's role as a key energy actor in the Black Sea will be significantly amplified. Starting from 2027, Romania is projected to become the European Union's largest natural gas producer, primarily through the full-scale exploitation of its offshore Neptun Deep project, operated jointly by OMV Petrom and Romgaz. This development adds a new layer of strategic relevance to the Black Sea, elevating Romania's position as a important energy supplier for EU partners such as Bulgaria and Republic of Moldova or even Germany, thereby further diminishing Russia's capacity to leverage energy dependence as a tool of regional coercion.

However, Romania's offshore expansion is unfolding in uniquely precarious conditions. Unlike other offshore developments in stable maritime environments, Romania's energy infrastructure is being constructed directly adjacent to an active war zone. The ongoing Russia-Ukraine conflict, and the potential reassertion of Russian naval power in the Black Sea in the event of a ceasefire that allows the Black Sea Fleet to fully return to Sevastopol, introduces considerable long-term strategic risks. Such a development could enable Russia to re-establish coercive leverage over the Western Black Sea, potentially threatening both Ukrainian naval operations and offshore energy installations, including those under Romanian jurisdiction.

The hybrid risk environment is further complicated by the pervasive threat posed by unexploded ordnance (UXO), which will continue to obstruct freedom of navigation and impede

[31] Zona Militar (2024). The First of the New Corvettes Built by Turkey for the Ukrainian Navy Underwent Live-Fire Tests, 18 November. Available at: https://www.zona-militar.com/en/2024/11/18/the-first-of-the-new-corvettes-built-by-turkey-for-the-ukrainian-navy-underwent-live-fire-tests/

offshore energy operations long after active hostilities cease. In this domain, the Baltic Sea states offer important institutional experience in UXO clearance and management, which could serve as a valuable template for Black Sea actors. Additionally, Ukraine's rapid development and operationalization of maritime drone technologies offers an innovative capability that could be adapted for Black Sea surveillance, mapping, and UXO identification missions. At the same time, the growing proliferation of Ukrainian-style maritime drones raises the risk of false-flag operations in the Black Sea, particularly as hybrid actors may employ drone copies to mask attribution and create escalation scenarios below the conventional threshold.

Given Romania's growing strategic centrality, both the EU and NATO will need to invest greater political attention into Black Sea cooperation frameworks. Romania's offshore production not only enhances regional energy security but simultaneously represents a high-value target for Russian hybrid pressure, given its potential to permanently reduce Moscow's energy dominance in Southeastern Europe. The UK and Norway-led Maritime Capability Coalition will become increasingly relevant as demining efforts intensify, a domain in which Romania is likely to play a leading operational role.

Finally, the establishment of the Black Sea Maritime Security Hub under the EU's 2025 Black Sea Strategy provides a valuable platform for advancing experimentalist governance principles in real-world operational settings. Through flexible, peer-informed cooperation between EU Member States, EEA partners such as Norway, and regional actors including Georgia and Türkiye, this emerging framework offers a unique opportunity to embed adaptive coordination mechanisms into the management of critical maritime infrastructure protection. In parallel, OMV Petrom's exploration of the Khan Asparuh perimeter, with the potential to transform Bulgaria into a net energy exporter, will further elevate the Black Sea's geopolitical profile, increasing both its strategic value and its exposure to hybrid threats.

In this respect, Romania can represent a testing ground where adaptive resilience mechanisms can be embedded as its infrastructure footprint expands. This forward-leaning approach not only enhances Romania's national security but offers transferable governance models that may be applied across contested maritime theaters within the broader EU and NATO frameworks.

4.2 Norway

What makes Norway interested in the question of protection of critical maritime infrastructure? First, critical maritime infrastructure is used to produce and export Norwegian energy

resources. Second, critical maritime infrastructure connects Norway with its main partners and energy clients in Europe as well as, through communication cables, with the rest of Europe directly, and via Europe with the rest of the world.

In 2024 the Norwegian petroleum sector that is the main operator of critical maritime infrastructure generated 21 percent of the country's GDP, 30 percent of the state revenues, absorbed 20 percent of investments and stood for 45 percent of the country's export revenues.[32] Norwegian subsea power cables play a part in securing the stability of the Norwegian electricity sector that is exposed to weather-related challenges due to its overreliance on hydropower.[33] Communication cables going via the North Sea connect Norway with other countries, give Norwegian actors direct access to various information services and in more general terms are the backbone of the internet, ensuring seamless global communication and economic activities, including international financial transactions and trade which is very important for a country with an open economy.

In the Norwegian expert debate critical infrastructure is understood as systems whose collapse can have serious negative impacts on functioning of the society (defence, welfare services, economic activity). Information and communication technology, power generation and distribution, gas and oil infrastructure, banks and other financial institutions, transport and water supply are defined as important elements of national critical infrastructure securing the smooth functioning of the state and society.[34]

The question of protection of critical infrastructure is approached from a functional perspective because infrastructure plays a crucial part in securing fundamental functions of the society and citizens' access to various critical services (Godzimirski 2021). Any element of infrastructure that is needed for performance of fundamental societal functions and meeting fundamental needs can therefore be defined as critical. Having this functional approach to critical infrastructure in mind it is understandable that to safeguard national security interests, it is crucial to identify what these fundamental national functions (FNF) are and to classify and protect infrastructure and objects worthy of protection based on this functional understanding. By the beginning of 2025 the list of FNF included 49 functions. Several of these FNFs play a

---

[32] https://www.norskpetroleum.no/en/economy/governments-revenues/

[33] For more on these issues see https://www.statkraft.no/kraftmarkedet-og-eksport-av-strom-via-utenlandskabler/ and https://energifaktanorge.no/en/norsk-energiforsyning/kraftmarkedet/.

[34] Ministry of Justice and the Police (2000). *St. meld. nr. 24 (1999–2000) Om sikkerhetspolitikk og beredskap* [White Paper No. 24 (1999–2000) On Security Policy and Emergency Preparedness]. Oslo: Norwegian Ministry of Justice and the Police.

part in safeguarding Norwegian national security interests in the maritime domain and Ministry of Energy has been assigned the overall responsibility for securing national power supply, transport of gas through pipelines to Europe, control of petroleum extraction on the Norwegian shelf and finally ensuring that the Armed Forces and pre-designated critical users have access to fuel.[35]

The current approach to protection of critical infrastructure is described in more detail in the new Law on Security from 2019.[36]This new law defines therefore elements of infrastructure that are worthy of protection.

One of the key innovations in the new 2019 Law on Security was more focus on protection against risks, challenges and threats stemming from cyberspace where one expects that various hybrid operations could be launched against critical infrastructure that has become increasingly digitized.[37] (Gjesvik 2019). This was justified by the fact that the 'interconnected nature of digital systems makes the risk of collateral damage and unintended consequences a serious concern'.[38]

The maritime elements of critical infrastructure include an extensive 8600 km long Norwegian system of gas pipelines managed and maintained by GASSCO, including three gas processing plants, some oil pipelines supplying oil to Europe, oil terminals from which oil is shipped to various customers by tankers and several power interconnectors linking Norway with English, Scottish, Dutch, Danish and German power grids. In addition, there are several communication cables connecting Norway via the North Sea with other countries and some petroleum installations with the Norwegian mainland.

To deal with the challenges related to protection of CMI several actions have been taken by various actors operating directly in Norway or having indirect stakes in the Norwegian CMI.

---

[35]NSM. Oversikt over innmeldte grunnleggende nasjonale funksjoner. Available at: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/

[36]Stortinget (2018). Lov om nasjonal sikkerhet (sikkerhetsloven) [Law on National Security]. Stortinget. Available at: https://lovdata.no/dokument/NL/lov/2018-06-01-24. For more on the implications of the new law, see: https://www.nsm.stat.no/publikasjoner/regelverk/lover/ny-sikkerhetslov-fra-1.-januar-2019/

[37]Gjesvik, L. (2019). Comparing Cyber Security: Critical Infrastructure Protection in Norway, the UK and Finland. NUPI. Available at: http://hdl.handle.net/11250/2598280

[38] Ibid., p.11.

To understand the Norwegian approach to protection of critical infrastructure, including CMI some attention must be paid to the concept of total defence. The core idea of the total defence concept is that only through involvement of Norwegian armed forces, cooperation between civil and military actors as well as support provided by allies will the country be able to deal with threats stemming from the whole threat spectrum. Operational measures implemented to protect critical infrastructure in the maritime domain involve various types of actors both in Norway and beyond the country's borders.

Corporate level

Equinor's and GASSCO's operations have been affected by negative trends in their strategic environment. The key elements of their infrastructure are defined as crucial for performance of fundamental national functions such as transport of gas through pipelines to Europe and control of petroleum extraction on the Norwegian shelf. Their operations and responsibility are therefore regulated by the new Law on Security which obliges them to implement various measures to mitigate risks and threats to their subsea infrastructure. To be able to protect their infrastructure they must have a good situational awareness and be able to deal with low scale threats, while responsibility for dealing with more serious threats is delegated to the country's military forces and other state institutions. An important measure implemented recently by Equinor in close cooperation with GASSCO is inspection of more than 7000 km of pipelines which has not discovered any substantial and intended damage and has therefore contributed to reducing Europe's concern for security of energy and gas supply.

State level

At the state level the work on protection of critical infrastructure is the responsibility of the Ministry of Justice and Public Security that has the overall responsibility for management of questions related to civil security, including protection of key objects and elements of infrastructure. The Ministry of Defence is responsible for the security of its own infrastructure systems. The Department of Public Security of the Ministry of Justice and Public Security is the main state organ coordinating the work on protection of critical infrastructure.

The fact that the state authorities decided to define transport of gas through pipelines to Europe and control of petroleum extraction on the Norwegian shelf as two of the 49 fundamental national functions has compelled the involved actors – Equinor and GASSCO – to implement adequate measures. Also the fact that the authorities have made the Ministry of Defence responsible for gathering relevant intelligence, improving situational awareness and

timely warning, handling of incidents and security policy crises and, if necessary, defending Norwegian or allied territory, as well as protecting Norwegian and allied forces, critical societal functions, and critical digital functions for the Armed Forces has improved the national ability to protect critical infrastructure.

In November 2024 Norway decided to join the international initiative on submarine cables.[1] This was an important step because most of Norway's communication with the outside world goes via such cables and by joining the statement, Norway will emphasize the importance of international cooperation in this field. The statement contains principles on security, reliability, interoperability, sustainability and resilience in connection with the planning, deployment, repair and maintenance of submarine cables.

Interstate level

Protection of subsea infrastructure, including Norwegian subsea infrastructure in the North Sea is of interest not only to Norway but also to other actors who could be negatively affected. This was most probably one of the key reasons why in April 2024 six North Sea countries: Belgium, the Netherlands, Germany, Norway, the UK, and Denmark decided to strengthen their cooperation in the region. The main objective of this cooperation is to protect subsea infrastructure in the North Sea through joining forces, taking appropriate measures and exchanging information and best practices. This initiative focuses on resilience and prevention and is therefore complementary to NATO's endeavours, which all participants involved are members of.[39]

NATO and the EU level

As mentioned earlier Norwegian authorities have adopted approaches to protection of critical infrastructure that are in line with the EU regulations and NATO expectations. These measures facilitate protection of critical Norwegian infrastructure that is also important to other actors such as the EU and NATO who have also embarked on closer cooperation to address various types of infrastructure related challenges. Because protection of critical maritime infrastructure has a clear transborder dimension and the EU and NATO are key security actors Norway welcomes all measures that will contribute to a better coordination of the cooperation between those two organisations on addressing infrastructure-related challenges in the time of

[39]Norwegian Government (2024). Six North Sea Countries Join Forces to Secure Critical Infrastructure. Norwegian Government. Available at: https://www.regjeringen.no/contentassets/03b6ba0be17e4ea0a57517a771ab5d8b/20240409_press-release_six-north-sea-countries-join-forces-to-secure-critical-infrastructure.pdf

increased tensions in the international environment in which Norway operates. It is clear that Norway's interests as the key energy provider to EU and NATO member states overlap with the interest in protection of critical infrastructure these two organisations have expressed. Some of these EU and NATO most recent measures aiming at addressing infrastructure-related challenges are described in the previous section of this report.

5. Regional Actions and Coordination

5.1 The Black Sea

While much of Northern Europe has already institutionalized multilateral hybrid threat coordination through mature structures like NORDEFCO and JEF, the Black Sea region remains comparatively underdeveloped in this regard. Rather than interpret this as a deficit, the governance vacuum creates a rare policy window. Romania's growing strategic importance, as both an emerging offshore energy hub and a full EU-NATO member, positions it to spearhead new governance architectures not bound by legacy institutional inertia. Infrastructural immaturity, paradoxically, allows Romania and its regional partners to embed adaptive, recursive governance frameworks from the outset.

Experimentalist Governance offers a particularly valuable framework for this context. Unlike rigid command-and-control models, EG accommodates institutional heterogeneity, permitting differentiated capacities while fostering voluntary coordination. Romania, Bulgaria, Türkiye, and Ukraine already exhibit partial experimentalist elements through localized adaptations in legal reviews, incident reporting, and situational awareness mechanisms. These existing national variations can serve as the foundation for cross-border peer-learning mechanisms, iterative coordination exercises, and gradually harmonized early warning and response protocols, all without necessitating formal, comprehensive treaty structures at this early stage.

Moreover, embedding experimentalist mechanisms early enables institutional learning before major hybrid disruptions fully materialize. Structured interoperability exercises, joint monitoring platforms, and common attribution benchmarks can gradually produce institutional memory and doctrinal reflexivity. In the longer term, this proactive model may serve as a template for broader NATO-EU hybrid threat coordination, one that balances sovereignty concerns with the operational imperatives of transnational critical maritime infrastructure protection in contested regions.

The governance gaps that characterize the Black Sea region do not solely constitute vulnerabilities; rather, they create a rare preemptive opportunity to embed adaptive governance frameworks before rigid sectoral structures crystallize. Romania, with its growing role as both an offshore energy hub and EU-NATO interface, is uniquely positioned to pilot experimentalist governance mechanisms. As critical maritime infrastructure expands, from subsea energy platforms to digital cable networks, early adoption of flexible coordination models, legal interoperability protocols, and regional peer-review processes can foster resilience from inception. This forward-leaning approach offers an alternative path to the fragmented and reactive governance trajectories seen in other contested maritime theaters.

5.2 Northern Europe

According to the most recent assessment of the situation presented by the Norwegian Ministry of Foreign Affairs in 2025 regional cooperation to safeguard peace and security has become more important. Norway's membership in NATO, but also the country’s connection to the EU, are of particular importance. Finnish and Swedish membership in NATO strengthens the opportunities for closer military and civilian cooperation, not least in the northern parts of the Nordic region.

Norway is involved in several layers of regional security cooperation. Being a relatively small country with limited resources, Norway supports the international order based on international law and the UN Charter. Norwegian membership in NATO is the most important regional and institutional framework for security provision. Although Norway is not a member of the European Union, it has a strong security partnership with the union and Norway has indeed defined several EU/European countries as strategic partners. In recent years, government documents have used the term ‘close allies’ systematically about the USA, the UK, Germany, the Netherlands, Denmark, Finland, Sweden and, increasingly, the Baltic states, France and Poland. Finally, cooperation on addressing various types of security challenges and issues with the Nordic countries is another regional form of cooperation prioritized by Norway, mainly under the NORDEFCO cooperation format, but now also inside of NATO structures following Finland and Sweden’s accession to the Alliance.

There are two regional frameworks for cooperation that shape the security situation in Northern Europe where all actors face a more assertive Russia. These are the NODEFCO framework

involving five Nordic countries (Sweden Denmark, Norway Finland and Iceland) and the Joint Expeditionary Force (JEF), involving all five Nordic countries and in addition the three Baltic countries, Lithuania, Latvia and Estonia, as well as the Netherlands and the UK that is the main coordinator of this cooperation.

NORDEFCO cooperation was launched in 2009. The main objective was to strengthen the participants' national defence, explore common synergies and facilitate efficient common solutions. The initiative emerged as an attempt to better structure Nordic security cooperation in response to unsuccessful experiences in Nordic cooperation. Finnish and Swedish NATO membership strengthens security of the whole region and has given a boost to NORDEFCO cooperation. The cooperation will be aligned with NATO's plans and doctrines. With Sweden and Finland in NATO the Nordic countries' strategic complementarities will strengthen the region's security. Collectively, the Nordic countries have the world's eleventh largest economy, 27 million inhabitants and, among other things, more than 250 modern combat aircraft. The expanding joint air operations is perhaps the foremost example of the combined potential of increased coordination and collaboration among the Nordic countries. in April 2024 the Nordic defence ministers signed a new NORDEFCO vision that takes this development into account. It states that a united Nordic region in NATO provides completely new opportunities for closer integration in the short term and across a wide range of areas.

NORDEFCO plays a significant role in enhancing the protection of critical infrastructure in the Nordic region and thus in the whole Northern Europe. NORDEFCO facilitates deeper defense cooperation among Nordic countries, which is crucial for protecting critical infrastructure. This includes joint operations, capability development, and security of supply. By coordinating joint procurement efforts, NORDEFCO ensures that member countries have access to necessary resources and technologies to protect critical infrastructure. NORDEFCO promotes civil-military collaboration, which is essential for safeguarding critical infrastructure against various threats, including cyber-attacks and physical disruptions. The cooperation provides a regional security framework that complements NATO's efforts. This is particularly important given the complex security environment in Northern Europe with the more assertive Russia as the key neighbour. NORDEFCO's Vision 2030 outlines long-term goals for defence cooperation, including the protection of critical infrastructure. This vision guides the collaborative efforts and ensures that they are aligned with current and future challenges. In addition, in response to Russia's invasion of Ukraine, NORDEFCO has strengthened its cooperation to address the broader security implications, which include protecting critical infrastructure and there are many infrastructure protection -related lessons to be learnt from the conflict in Ukraine where Russia has launched massive attacks on national critical infrastructure. NORDEFCO cooperation is

therefore vital for ensuring the resilience and security of critical infrastructure in the Nordic region, thereby contributing to overall regional stability.

All Nordic countries take part in the UK-led Joint Expeditionary Force (JEF) initiative established in 2014, which is a military partnership between a smaller group of countries in Northern and Western Europe. JEF constitutes a framework for close cooperation between like-minded Nordic and Northern European countries and plays an important role both as a political consultation forum and as an operational framework. JEF is primarily a regional resource in peacetime that can also respond quickly to emerging crises at an early stage, which makes a seamless transition from a coalition operation to an allied operation possible.

The Joint Expeditionary Force (JEF) plays a significant role in protecting critical infrastructure, particularly in Northern Europe. The JEF conducts protective military activities to secure critical undersea infrastructure, such as energy and communication cables. For example, the JEF's NORDIC WARDEN exercise involves ships, aircraft, and personnel from JEF nations to monitor and protect undersea routes. In response to incidents like the damage to the Balticconnector gas pipeline, the JEF activates Joint Response Options (JROs). These include exercises and patrols to enhance the security of undersea infrastructure in areas like the Baltic Sea and the Norwegian Sea. The JEF supports NATO's efforts by providing additional surveillance and reconnaissance capabilities. This includes monitoring shipping activity near critical undersea routes and coordinating the detection of suspicious activities. The JEF's activities contribute to a broader regional security framework, ensuring that critical infrastructure remains resilient against potential threats. This is particularly important given the strategic significance of undersea infrastructure for economic and military operations.

6. Policy Recommendations

6.1 Standardized Protocols and Pre/Post-Attack Preparedness

In the context of hybrid threats targeting critical maritime infrastructure (CMI), standardization of protocols across sectors and agencies is essential. These threats rarely appear as singular, high-impact incidents. Hybrid actors exploit “infinite iteration” logic[40], relying on the cumulative effect of frequent, low-grade actions such as GPS spoofing, cable probing, or sensor disruption. While individually deniable and below escalation thresholds, these actions

[40] Balcaen, Du Bois and Buts (2021). A Game-Theoretic Analysis of Hybrid Threats

undermine infrastructure resilience over time, exhausting detection systems, legal clarity, and institutional response cohesion.

This operational environment demands forward-leaning SOPs, not only for direct response but for anomaly escalation and cross-agency continuity. Robust pattern recognition, horizontal incident linking tools, and shared repositories of institutional memory are essential to detect connections between low-intensity incidents that may otherwise appear isolated. Without procedural readiness and shared analytical frameworks, strategic degradation can unfold without triggering any one institution's threshold for action.

To this end, the paper recommends the implementation of pre- and post-attack integration protocols. Effective response to hybrid operations requires a tri-layered framework that merges technical analysis, legal readiness, and economic impact mitigation.[41] Before a crisis unfolds, preemptive legal reviews of CMI systems should be conducted to determine the response boundaries and liability risks. In the aftermath of an incident, WP2 proposes a cyber-legal-economic triage playbook, designed to manage ambiguity, ensure operational continuity, and clarify attribution responsibilities. Such a framework should be embedded within a wider ecosystem of SOPs capable of supporting multi-agency, cross-sector response.

In conclusion, defending CMI from hybrid threats cannot rely on technical defenses alone. Instead, standardized, cross-sectoral protocols must serve as the connective tissue that ensures continuity, accelerates escalation when needed, and builds resilience across maritime, legal, and institutional domains.

6.2 Command Structures and Crisis Team Design

In the face of hybrid threats, especially those targeting time-sensitive and geopolitically exposed assets such as offshore energy platforms or undersea communication cables, operational response structures themselves must adopt experimentalist features. Traditional command structures, centered on fixed hierarchies and rigid role definitions, are ill-suited to respond effectively under ambiguity. Instead, command and control (C2) models must be modular, recursive, and able to shift fluidly across multi-agency configurations depending on

[41]Mazaraki and Goncharova (2022). Cyber Dimension of Hybrid Wars.

the nature, tempo, and escalation path of hybrid threats. Such adaptive architectures can enable coordinated decision-making without sacrificing flexibility.[42]

In the face of hybrid threats, especially those targeting time-sensitive and geopolitically exposed assets such as offshore energy platforms or undersea communication cables, operational response cannot be rigid or top-heavy. Traditional command structures, centered on centralized, hierarchical control, may prove too slow or siloed to respond effectively in ambiguous, fast-evolving hybrid scenarios. Instead, as Bakken, Hærem, and Lund-Kordahl (2025)argue, command and control (C2) models must be dynamic, able to shift fluidly between centralized and hybrid configurations depending on the nature, tempo, and escalation path of the threat.

Such hybrid command structures must be pre-designed to accommodate multi-agency collaboration, particularly between civilian, military, and private-sector actors. For instance, a cable sabotage incident may initially fall within the operational remit of a private operator or coast guard unit, but could quickly require escalation to naval or intelligence units as evidence of foreign interference mounts. In this scenario, rigid role definitions can lead to fragmented micro-management, delaying containment or attribution.[43] Therefore, WP2 advocates for C2 ecosystems that anticipate role-switching, co-location, and information-sharing across previously unconnected organizational silos.

Equally important are the soft factors that underpin successful crisis coordination. Psychological safety, the belief that one can raise concerns, ask questions, or redirect response without fear of blame., is essential for inter-agency trust and rapid adaptation. Designing SOPs and training environments that promote trust, communication clarity, and learning culture are the foundation for sound crisis coordination. Such conditions make it possible to identify informal leadership, uncover coordination bottlenecks, and ensure that civilian, military, and commercial actors function as a cohesive unit even under high ambiguity.

Ultimately, building effective CMI defense teams is not just about doctrinal clarity or technical tools, it is about designing flexible command structures that can adapt in real time and embedding them with organizational cultures capable of functioning in the gray zone. Only

---

[42]Bakken, T., Hærem, T. and Lund-Kordahl, I. (2025). Building Competence Against Hybrid Threats: Training and Exercising Hybrid Command Organizations. In: Borch, O.J. and Heier, T. (eds.) Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response. Routledge.

[43] Borch and Heier (2025). Toward a Hybrid Threat Response Model.

such models can withstand the distributed, iterative, and unpredictable nature of hybrid threats in the maritime environment.

6.3 Training, Exercises, and Competence Building

In the context of hybrid threats targeting CMI, training cannot be linear, prescriptive, or domain-isolated. Instead, it must reflect the Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) of the hybrid threat environment.[44] Maritime crisis teams must be trained in realistic, inter-agency environments that mirror the fluidity and fragmentation of gray zone operations. Simulations must test not only technical responses but also situational awareness, communication under stress, and the emergence of informal leadership structures.

To enhance the realism and analytical value of such exercises, AI-driven red teaming and immersive VR simulations should be integrated. These tools allow for the replication of complex sabotage scenarios, cyber-physical disruption sequences, and ambiguous incident escalation paths. By creating controlled settings in which institutional blind spots can be observed and addressed, these simulations offer a scalable method to stress-test CMI protection protocols and identify areas of operational friction.[45]

Traditional instructional models, based on fixed objectives, sequential drills, and predictable environments, are increasingly obsolete in this space. Recent literature[46] argues for a hermeneutical approach to pedagogy, in which learning is based on interpretation, reflexivity, and awareness of cognitive blind spots. Such pedagogy fosters meta-competence, the ability to learn how to learn, adaptively, across unpredictable contexts. Their strategic education frameworks (PED-PREP and HE-HYB-PEP) provide a roadmap for developing long-term adaptive competence, not just procedural proficiency.

Finally, competence building must be paired with institutional knowledge development. As Borch & Heier (2025) argue, operational preparedness requires both short-term intelligence for early warning and long-term learning loops that refine doctrine, reshape training, and feed back into strategic planning. Multi-source surveillance systems and pedagogical openness to cross-

---

[44] Bakken, Hærem and Lund-Kordahl (2025). *Building Competence Against Hybrid Threats*.

[45]Idem.

[46]Magnussen, L.I., Torgersen, G.-E., Boe, O. and Saeverot, H. (2025). Competence for Hybrid Threats: A Strategic Competitive Development Model. In: Borch, O.J. and Heier, T. (eds.) Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response. Routledge.

sector feedback are essential for interpreting hybrid anomalies—not just detecting them. Training must be cyclical, reflexive, and embedded in the broader institutional system of resilience.

6.4 Infrastructure-Centric Defence Architecture

As hybrid threats increasingly target the infrastructure layer of maritime security, pipelines, undersea cables, offshore platforms, and port systems, protection efforts must balance technical safeguards with adaptive governance structures. Rather than relying on rigid pre-defined protocols, defense planning should adopt multi-layered architectures that serve as modular platforms for iterative coordination, flexible adaptation, and peer-informed governance. Dimitrov & Karakolev[47] offer one such scalable blueprint, which can serve as an evolving reference framework for safeguarding CMI within experimentalist governance cycles. Each of these layers offers a functional domain in which experimentalist governance cycles can operate, allowing cross-sector actors to co-develop adaptive measures, refine protocols, and update defensive postures in response to evolving hybrid tactics.

1. Physical Protection

The first line of defence involves physical hardening of infrastructure components. Methods such as burial, trenching, sheathing, and rock dumping reduce vulnerability to direct sabotage or environmental degradation. Materials like carbon steel with concrete coatings are recommended for underwater pipelines and cables, adding resilience against both hostile interference and long-term corrosion.

2. Technological Protection

Physical measures alone are insufficient without persistent situational awareness and early warning systems. The second layer of defence involves the deployment of autonomous systems (USVs, AUVs, drones) for wide-area monitoring, combined with sensor integration, including acoustic, infrared, satellite, and underwater communication arrays. These are supported by robust cybersecurity systems: SCADA protection, intrusion detection systems (IDS), and AI-driven predictive maintenance tools, which help to detect anomalies before

[47]Dimitrov, N. and Karakolev, K. (2024). Seabed Critical Infrastructures. Information & Security: An International Journal, 55(2), pp. 133–148. Available at: https://doi.org/10.11610/isij.5566

they escalate into critical failures.

3. Operational and Procedural Layer

The third layer focuses on cross-sectoral crisis response. This includes multi-agency incident protocols, real-time alert mechanisms, redundancy planning, and the operational integration of naval, coast guard, and private operators. Case studies from Norway illustrate how public-private coordination mechanisms can enable rapid mobilization and information sharing. In a hybrid threat scenario, this layer determines whether an incursion is contained quickly—or allowed to escalate through indecision and procedural fragmentation.

4. Legal and International Cooperation Layer

The final layer of the model addresses the normative and regulatory environment that underpins infrastructure defence. It emphasizes the need to harmonize national legal frameworks with international ones, combining UNCLOS, IMO regulations, EU directives (e.g. Directive 2013/30/EU), and national legislation. Dimitrov & Karakolev[48] advocate for joint surveillance initiatives and NATO-aligned information-sharing protocols, ensuring that incidents affecting shared infrastructure are not addressed in isolation.

Legal resilience also requires acknowledging strategic trade-offs. Norm-based deterrence strategies, anchored in the language of the rules-based international order (RBIO), can inadvertently constrain strategic flexibility.[49] Public commitments to uphold legal norms may lead to rhetorical entrapment, where states are held to symbolic consistency even when facing ambiguous or hybrid threats. This risk is evident in the Estonia–Finland response to recent Baltic Sea infrastructure incidents. While both countries were quick to attribute the damage to external actors and frame the events within the logic of hybrid aggression, they simultaneously emphasized legal restraint and downplayed immediate retaliatory measures. This underscores the strategic tension between projecting normative clarity and preserving operational adaptability.[50]

---

[48] Dimitrov and Karakolev (2024). *Seabed Critical Infrastructures.*

[49] Strating, R. (2021). *The Rules-Based Order as Rhetorical Entrapment: Comparing Maritime Dispute Resolution in the Indo-Pacific*. Contemporary Security Policy, 42(3), pp. 372–409. Available at: https://doi.org/10.1080/13523260.2021.1901818

[50] Ibid.

Together, these four layers form a comprehensive operational framework that transforms CMI protection from an abstract resilience goal into a structured set of defendable domains. The paper recommends this architecture as a baseline template that can be adapted by national authorities, infrastructure operators, and regional coalitions seeking to counter hybrid maritime threats. Importantly, while these layers provide an operational starting point, their real resilience value lies in being continuously updated, reviewed, and recalibrated through recursive learning processes and peer-informed coordination mechanisms, core features of Experimentalist Governance discussed throughout this study.

6.5 Surveillance

Hybrid threats are designed to evade conventional detection and attribution frameworks. They often appear as technical anomalies or isolated incidents, but are in fact strategically timed and layered.[51] Traditional cyber threat attribution techniques, focused on technical signatures like IP addresses or malware code, are easily obfuscated and therefore inadequate in the hybrid context. Defending critical maritime infrastructure (CMI) requires not just smarter surveillance tools, but a different analytic paradigm: one that links technical forensics with behavior and context.

To achieve this, hybrid threat analysis must be recalibrated to incorporate what Irshad & Siddiqui describe as hybrid features:

> Technical (e.g., malware type, TTPs),
>
> Behavioral (e.g., attack timing, repetition, target profile), and
>
> Geopolitical context (e.g., regional tensions, known adversary patterns).

These elements, when fused, allow for the emergence of a context-aware approach to attribution, where anomalies are not merely flagged, but interpreted as strategic signals. This approach demands integration with regional intelligence, historical conflict data, and adversary behavioral profiles.

[51] Irshad and Siddiqui (2024). *Context-Aware Cyber-Threat Attribution*

At the system level, enabling such interpretation requires governance-ready data ecosystems. Pestana & Sofou[52] propose four foundational pillars for this:

> 1. Common Standards and Definitions, to ensure interoperability between CMI operators, government agencies, and alliance partners;
>
> 2. Integrated Information Sharing Mechanisms, to support rapid attribution and response;
>
> 3. Cross-sectoral Trust Mechanisms, to reduce siloed threat reporting and encourage real-time collaboration; and
>
> 4. Investment in Data Literacy and Skills, to ensure that tools are matched with institutional competence.

Surveillance infrastructure without analytical context and data governance is functionally blind. Conversely, even the most advanced analytic tools cannot support deterrence if they operate in legal or policy vacuums. For example, the absence of viable insurance schemes for hybrid cyberattacks on CMI introduces unacceptable financial opacity, weakening private sector incentive alignment. EU or NATO-backed risk-pooling mechanisms or public-private insurance frameworks would both reinforce economic resilience and elevate the deterrent posture of private operators[53]. In other words, economic visibility is part of strategic visibility. Ultimately, the study frames technology not just as a surveillance asset, but as a strategic enabler for resilience and attribution. Tools for denying deniability must be embedded in interoperable systems, trained on hybrid-aware data inputs, and governed by protocols that integrate private, public, and multilateral stakeholders into a shared threat picture.

6.6 Black Sea-Specific Experimentalist Governance Recommendations

Policymakers should leverage the early-stage development of Black Sea infrastructure to integrate Experimentalist Governance models before rigid sectoral silos emerge. Unlike regions where institutional complexity often inhibits adaptive reforms, the Black Sea's relatively nascent governance architecture creates space for proactive rule-making. Mechanisms such as joint

[52]Pestana, G. and Sofou, S. (2024). Data Governance to Counter Hybrid Threats Against Critical Infrastructures. Smart Cities, 7(4), pp. 1857–1877.

[53]Goncharova and Mazaraki (2022). *Cyber Dimension of Hybrid Wars*

incident reporting cells, peer-review attribution panels, and voluntary legal Standard Operating Procedure (SOP) exchanges should be piloted in parallel with infrastructure deployment, allowing cross-sectoral coordination to evolve in tandem with physical assets.

Romania should assume a convening role by launching modular working groups under both EU-NATO auspices and complementary regional formats. These platforms can accommodate the diverse legal frameworks, alliance commitments, and operational capacities that characterize Black Sea littoral states. This incrementalist, peer-informed approach to hybrid threat coordination fosters gradual convergence without prematurely imposing rigid harmonization, thus balancing national sovereignty concerns with collective resilience-building imperatives.

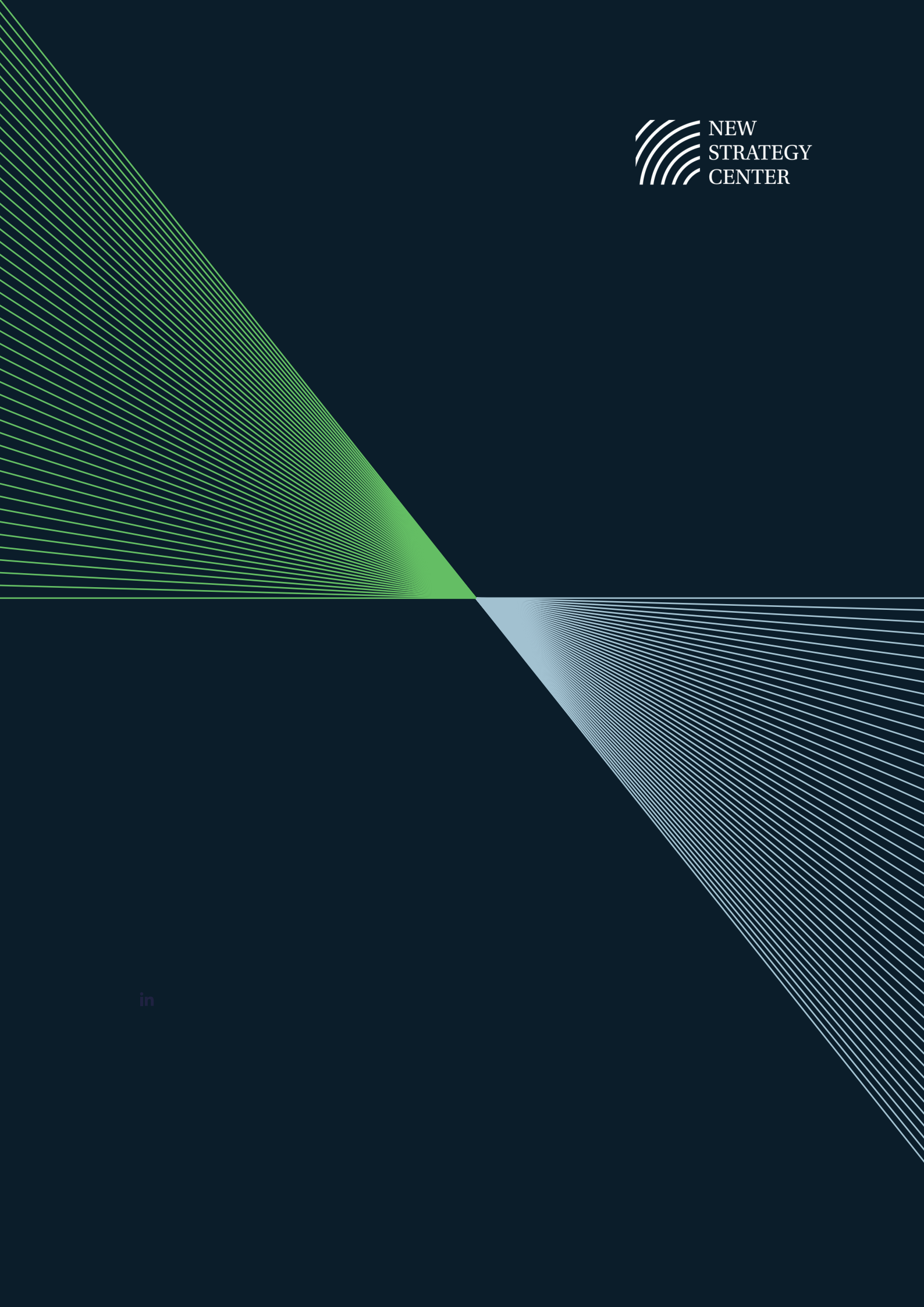
As Romania expands its offshore energy portfolio, including projects such as Neptun Deep, early-stage legal and operational frameworks must address the dual-use dilemmas inherent in maritime infrastructure. Proactive governance should clarify the balance between civilian exploitation, military signaling, and hybrid threat vulnerability mitigation. The adoption of adaptive legal protocols at this stage not only strengthens Romania's national posture but offers a scalable model for managing hybrid pressures in contested maritime zones globally.

7. Conclusion

This study has argued that safeguarding maritime critical infrastructure in an age of hybrid threats requires more than technical reinforcement or reactive coordination. It demands a rethinking of governance itself. By drawing on the principles of Experimentalist Governance (EG), this paper has offered a scalable, adaptive framework for designing protection architectures that can evolve with the threat landscape.

The North Sea serves as a functional reference point, with a strong governance eco-system. Yet it is in the Black Sea, where hybrid pressure converges with underdeveloped governance ecosystems, that the need for institutional innovation is most urgent. Romania, with its expanding offshore infrastructure and unique dual anchoring in the EU and NATO, emerges as a credible laboratory for testing new governance models under real-time pressure. Its partnerships with Bulgaria, Türkiye, Ukraine, and broader Euro-Atlantic actors point to the feasibility of flexible, modular cooperation mechanisms beyond formal legal harmonization.

Rather than prescribing fixed doctrines or universal templates, this study advocates for recursive learning, voluntary interoperability, and modular architecture—an approach that aligns resilience-building with the very fluidity hybrid threats exploit. While the North Sea illustrates how institutional maturity enables infrastructure resilience, it is the Black Sea's volatility that offers a proving ground for adaptive governance. With the right institutional mindset, contested waters like the Black Sea can become frontlines of experimentation.


NEW
STRATEGY
CENTER