Europe's Maritime Security Dilemma – Critical Maritime Infrastructure

2 NOVEMBER 2026

Kuzey Tunguz



Baltic Sea and a vessel on NATO patrol mission

Opening Points

Following Russia's 2022 invasion of Ukraine, the Baltic Sea has again become a central domain for European security concerns. This is driven both by its importance for conventional military reinforcement and maritime supply routes, and by the region's vulnerability to ambiguous, deniable, and disruptive actions targeting undersea and maritime infrastructure (Castrogiovanni, 2026). Early conceptions of hybrid warfare focused on adversaries who blend conventional military power with irregular tactics, terrorism, and criminal activity in a shared operational space, combining these elements to produce compounded effects against militarily superior enemies. Today, it is observable that the domain of hybrid warfare has expanded into the far utilisation of civil means, in particular, addressing this paper, supply chains and maritime zones.

Security Perception

European countries' feeling of an Eastern threat is not subjective but an inevitable aspect of the state. If a state's assets were in jeopardy, particularly by a third party, an incident would trigger a preventive mechanism in order to counter or retaliate. Today, after the Russian-Ukrainian war, the Western bloc increased its measures against the Russian threat. Russia is perceived as a threat to the existing order in continental Europe. Incidents in the Baltic Sea showed the scale to which security-oriented fears are imminent.

Hypothetically, a coordinated strike on various critical infrastructure assets in the Baltic Sea could result in direct repair costs and immediate economic losses ranging from tens to hundreds of millions of euros, alongside a risk of billions in broader economic disruption if several electricity, telecommunications, and energy connections were to become unusable at the same time. The EstLink 2 incident serves as a valuable reference; the initial significant failure allegedly needed around €30 million for repairs and led to an estimated €94 million in extra costs for consumers in Estonia and a later outage incurred around €50–60 million in repair expenses (European Commission, Directorate-General for Energy, 2025).

The economic and energy security of Europe is critical, but in such a scenario, there is an unquantified cost to the public today: strategic security and escalation costs. If an attack were to occur, European governments must simultaneously protect existing infrastructure, ensure energy and communications systems remain operational, deploy naval and surveillance resources, and establish accountability for the attack. That would amount to almost a mass mobilisation of nations, creating shock waves through continents' economies and social structures. It is significant to assess how each nation's reaction, in this case, restructuring public roles, wartime law or measures, would impact the overall well-being of European countries. Secondly, if there were to be an attack on infrastructure to paralyse Western society, would retaliation escalate into a total annihilation of the World? Well, though answers remain unpredictable, it raises the question of "how does Russia perceive hybrid attacks as a means of imposing strategic costs on Europe while remaining below the threshold of conventional war?"

To further illustrate the means and ends to gain a rational perspective in terms of "loss/benefit" or "trade-off", understanding the use of hybrid means by Russia is fairly significant to provide a meaningful analytical framework. Russian strategic thought stays grounded in traditional concerns of warfare, strategy, and state survival, rather than treating hybrid tactics as some new, all-encompassing toolkit in their own right. Seen this way, hybrid methods represent just one piece of a wider Russian approach to conflict. Russian art of war views war and peace not as distinct states, but as points along a single continuum (Monaghan, 2015).

The inflection between converging sides, Praks (2024), argues that the Russian government perceives its war in Ukraine as an element of a broader

worldwide struggle with the "Collective West." President Putin has linked his domestic legitimacy and the reorganisation of the Russian political and economic framework to a significant geopolitical clash with the West, claiming the latter is conducting a "hybrid war" against Russia (Praks, 2024). These conflicting views among counterparts reflect not only the nature of conflicting views, but also the reality of perception of the other.

Baltic Sea and Security Dynamics

The Baltic Sea has emerged as one of Europe's most contested security arenas, with evolving conflict dynamics reshaping regional collaboration, especially since Sweden and Finland joined NATO. The Danish Straits remain vital maritime chokepoints, governed by customary international law and the 1857 Copenhagen Convention, in contrast to the Turkish Straits, which are governed by the Montreux Convention. Their toll-free transit system also raises concerns about access limitations and potential shutdowns during emergencies (Pribyl, 2026).

Russia is generally believed to be responsible for a number of recent incidents involving damage to undersea cables and pipelines, despite no official determination of state accountability by the authorities investigating these incidents. The initial sign that Baltic Sea Critical Undersea Infrastructure (CUI) could be at risk of sabotage emerged in September 2022, following the explosion-induced breakage of the Nord Stream pipelines. From October 2023 to January 2025, approximately 12 pipelines and power and communications cables (likely including at least two Russian cables) were cut in four distinct anchor-dragging events, with three occurring between November 2024 and January 2025 (Lawrence et al., 2025).

The hybrid threat spectrum, hence, extends into critical infrastructure embedded within the Baltic Sea, which showed its vulnerability to sabotage in 2022. Pribyl (2026) further illustrates how the seabed of the Baltic contains essential telecommunications cables, power connections, and gas pipelines, rendering it susceptible to interference by opponents aiming for economic or strategic impacts without reaching the level of armed conflict.

Critical Maritime Infrastructure

The increasing susceptibility of essential maritime infrastructure blurs the lines between peace and warfare, with both state and non-state actors exploiting new vulnerabilities. The mainly private ownership and spatial distribution make it difficult to monitor, deter, and assign responsibility for hostile actions. Furthermore, the diversity of maritime infrastructure, whether related to critical energy or data cables, also determines the extent to which redundancy can be mitigated. Per se, energy security becomes an evident aspect of national and regional security, which may suggest stronger state involvement in these sectors. Also, it is important to bear in mind that the global aim of transforming to low-carbon energy might be

an overwhelming trajectory, as hybrid warfare threatens to undermine such efforts point-blank (Neal, 2026).

The legal intricacies of the ocean under UNCLOS (United Nations Convention on the Law of the Sea) lead to considerable ambiguity. Coastal nations possess resource rights within their EEZs, yet states maintain wide-ranging liberties, which simply suggests that actions like surveillance or cable-tapping are not consistently banned. However, for the non-state actors, the circumstances vary, as their conduct is primarily governed by the domestic regulations of coastal or flag nations. The Nord Stream sabotage highlighted these issues, prompting Germany, Denmark, and Sweden to initiate independent criminal inquiries (Neal, 2026).

European Response to Emerging Maritime Threats

Following a period of mild disregard, European NATO and EU nations are re-engaging in naval capabilities, primarily due to the recapitalisation occurring alongside Europe's overall shift towards defence and security. Simultaneously, the insights gained from the rapid shifts on the battlefield in Ukraine are challenging Europe's capacity to adapt to advancing military technology as it endeavours to take on a larger share of its defence responsibilities. Furthermore, the United States anticipates a new 'burden sharing' framework in which European allies take on primary responsibility for security in Europe. This involves a decrease in its role as a conventional source of essential naval capabilities and encourages Europeans to bureaucratize investment in reinforcement (Childs & Fischbach, 2026). Ad hoc efforts toward a common framework to secure continental Europe, in this paper's case maritime, significantly elevated the capabilities and posture of both military and civil means against naval threats.

The EEAS (2026) aims to bolster European maritime security by increasing naval operations, fostering closer ties with NATO and coast guards, forming international partnerships, improving maritime awareness, and developing joint capabilities to address conventional, cyber, and hybrid threats. (EEAS, 2026).

Today, the rise of maritime disputes is not coincidental but rather the result of exploitation. In the Baltic Sea, at least 11 incidents involving underwater cables and pipelines occurred over 15 months, prompting NATO to establish Baltic Sentry to safeguard essential infrastructure. And in the Black Sea, Ukraine has used a fleet of low-cost uncrewed surface vessels to drive a conventional navy against and attempt to disrupt commercial trade routes in the region (Laird, 2026).

Notably, none of these situations constitutes a traditional military conflict in the Cold War sense; however, each is highly likely to utilise unconventional methods. Laird (2026) further illustrates that this very threat trend uses the same structural vulnerability, an Maritime Domain Awareness framework which was formulated to identify and count acknowledged

governmental bodies. However, MDA faces challenges in interpreting the motives of unclear, deniable, or non-state actors operating in civilian maritime spaces and exploiting legal domains that grant civil rights (Laird, 2026; Neal, 2026).

Concluding Points

Neorealist theorists reinterpret the security dilemma as a structural, state-centred aspect of international anarchy, highlighting systemic limitations and downplaying the significance of agency or perception. Mearsheimer's concept of 'offensive realism' views the dilemma as 'tragic' and inescapable, whereas others suggest it arises from uncertainty regarding intentions. Critics such as Eric Van Rythoven argue that this perspective overlooks the significance of human factors, decentralising the subject into various subactors (Mearsheimer, 2001; Van Rythoven, 2016).

Scholars, particularly Jennifer Mitzen and Brent Steele, broaden the security dilemma by emphasizing the necessity for states' ontological security; A consistent identity and continuity drawing attention to the significance of perception and internal assurance. Although this perspective still primarily centres on the state and is less applicable to the multi-actor environment of hybrid threats and CMI, the politics of constructing threats, or securitisation, complicates the security dilemma, as attempts to garner backing may backfire or lead to new vulnerabilities (Neal, 2026).

Future reference on maritime threats in the Strait of Hormuz provides valuable insights. Iran has shown that the mere threat of shutting down or disrupting traffic can be used as a bargaining chip, compelling opponents to consider the economic impacts of escalation. Russia would likely see any effort to limit access through the Danish Straits as an act of war. Though CMI remains at the core of the prosperity of continental Europe regardless of naval strength, advances in technology provide innovative methods for asymmetric threats against conventional structures. Per se, Russia's capacity to jeopardise Baltic trade poses a strategic weakness that NATO and the EU must confront with innovative methods. This paper emphasises the need for further research into how to tackle rising hybrid threats to national security within the power dynamics, within the scope of this paper's range: maritime security and CMI.

References

Childs, N., & Fischbach, J. R. (2026, June 16). *Baltic and northern defence: Towards an integrated maritime strategy*. Konrad-Adenauer-Stiftung.

European Commission, Directorate-General for Energy. (2025). *EU energy security – Evaluating the EU's security of electricity and gas supply framework* (SWD(2025) 435 final).

Pribyl, S. (2026, August 11). *Securing the Baltic: The strategic imperative for a comprehensive maritime security strategy*. Center for Maritime Strategy.