INFO FLASH
Finabel
The European Land Force Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

NOVEMBER 2024


**WRITTEN BY**
NICOLA BARBESINO

**EDITED BY**
CATERINA PANZETTI

**SUPERVISED BY**
VICTORIANO VICENTE BOTELLA BERENGUER

## Introduction

The events following the 2022 Russian full-scale invasion of Ukraine have reshaped the political and military landscape of Europe. Rising geopolitical tensions between the Russian Federation and NATO-EU countries have marked the increasing strategic importance of the Nordic-Baltic region as a potential space for confrontation. Against this backdrop, the Baltic and Nordic seabed has emerged as a critical strategic battlefield for Russian hybrid tactics to asymmetrically influence European security and destabilise NATO members' societies and states. Beneath the waters of the Baltic Sea, the network of undersea cables and submarine infrastructure is now at the centre of the battlefield preparation between Russia and the European Allies.

Relevantly, undersea cables form the backbone of international connectivity and represent a vital element for worldwide communication and the global economy. More than 95% of all internet transfers run through about 500 submarine cables stretching over 1.4 million kilometres under the world's oceans (Chataut, 2024). A daily financial traffic of approximately $10 trillion in transactions, military communications, and power grids all critically depend on the continuous operation of this network. Attacks or damages to even parts of these networks of cables would result in catastrophic disruptions for the private and government sectors across the globe (Bueger et al., 2022).

This study looks at the wider Baltic region to assess the importance and the vulnerabilities of critical undersea infrastructure within the context of an increasingly tense strategic landscape in Europe. The fragility of submarine cables in the Baltic and North Seas has a direct impact on the security of European states and the telecommunication needs of our advanced societies. The defence and resilience of critical undersea infrastructure have steadily moved to the forefront of Allied strategic planning due to the heightened concerns over Russian capabilities and willingness to degrade and destroy submarine cables and pipelines within Moscow's overarching hybrid way of warfare. The first section of this paper looks at the established international legal framework of undersea cables before turning to the regional governance of the Baltic seabed to evaluate the lack of adequate legal protection to counter aggressors. Subsequently, the paper outlines a comprehensive overview of the existing threats to submarine infrastructure. Finally, the last section delves into the grey zone dynamics and military capabilities of Russia and NATO in the undersea domain of the wider Baltic region.

## 1. The legal ambiguity of the (under)seascape and cable network governance in the Baltic Sea

The transnational undersea networks forming the physical bedrock of all digital traffic and global communications––including private calls and emails, financial data and governments' sensitive intelligence––are primarily financed, owned, and operated by private businesses. Indeed, commercial entities control cable routes and connections despite the crucial importance of sub-sea infrastructure to states' national security and strategic interests (Solarz Hendriks & Halem, 2024; Bashfield, 2024). This lack of state oversight and ownership makes the international legal framework concerning the sub-sea maritime domain convoluted and inadequate for the modern-day governance of undersea cables in a contested geopolitical environment (Sunak, 2017). Thus, it is critical to understand the regulatory system surrounding these cables, starting from the landing stations and the territorial waters, before moving to the more tangled body of international law.

While it is evident that the onshore landing sites and the segments of undersea cables falling within the territorial sea are subject to the state's sovereignty, the protection of undersea cables in the Exclusive Economic Zone (EEZ) is not as well established. Only a few countries have extended the jurisdiction to safeguard undersea maritime infrastructure to the EEZ, and none of the Baltic and North Seas coastal states. Generally, these measures take the form of restricted areas banning shipping and fishing activities along cable routes to prevent or minimise accidental damage to the infrastructure. For instance, New Zealand and Australia established Cable Protection Zones (CPZs) in 1996 and 2007, respectively (Sunak, 2017). These submarine cable protection regimes restrict potentially dangerous activities and criminalise cable damage (Bashfield, 2024). In the Australian case, the CPZs extend up to 40 nautical miles offshore and up to a depth of 2,000 metres, with possible prison terms for entities engaging in illegal activities in the protection zones (Australian Government, 2024).

When considering the legal status of undersea cables under international law, three major multilateral agreements dealing with the sub-sea domain stand out: the 1884 Convention for the Protection of Submarine Telegraph Tables, the 1958 Geneva Convention on the High Seas, and the 1982 United Nations Convention on the Law of the Sea.

The Convention for the Protection of Submarine Telegraph Cables, signed in 1884 by 36 state parties, represents the first multilateral treaty to specifically address the protection of submarine communication cables (NATO CCDCOE, 2019). Article II considers it a punishable offence to "break or injure a submarine cable, wilfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication" (Convention for the Protection of Submarine Telegraph Cables, 1884). However, with Article XV, the 1884

Convention clarifies that the provisions do not apply in case of armed conflict (NATO CCDCOE, 2019): "The stipulations of the present Convention do not in any way restrict the freedom of action of belligerents" (Convention for the Protection of Submarine Telegraph Cables, 1884). Accordingly, the United Nations Convention on the High Seas, signed in Geneva on the 29th of April 1958 by 46 countries, affirmed in Article 27 that every state party to the treaty "shall take the necessary legislative measures" to make the breaking of submarine infrastructure in the high seas a punishable offence (Convention on the High Seas, 1958). Whilst the 1958 Geneva Convention provided for cases of wilfulness and negligence, it still failed to fully address the instance of deliberate damage by a hostile actor (Sunak, 2017; NATO CCDCOE, 2019). Subsequently, in 1982, the United Nations Convention on the Law of the Sea (UNCLOS), often referred to as 'the Constitution of the Sea' due to the signatory of 167 state parties, achieved considerable progress in the protection of undersea cables in international waters (Sunak, 2017). Despite added legal protections in the form of Article 113, which requires states to enact national laws to punish the breaking of cables, UNCLOS does not extend an international protection regime to submarine cables during wartime (Sunak, 2017). Established state practice since the 1884 Convention is to consider undersea cables as legitimate targets in military operations. Furthermore, Article 113 of UNCLOS does not clearly allow navies to board and search vessels in international waters suspected of interfering with undersea infrastructure (Kaushal, 2023).

Ultimately, one can conclude that the safeguards and protection mechanisms of maritime sub-sea infrastructure enshrined in existing international law are ill-equipped and outdated for the crucial role that undersea cables play in the digital age vis-à-vis the 1970s and 1980s. This poses fundamental challenges to protecting submarine infrastructure from hostile actors not only above the threshold of war but also during peacetime grey zone operations.

Having analysed the legal status of undersea cables in international law, one must adopt a regional perspective on the governance of sub-sea maritime infrastructure considering the specific geopolitical features of the Baltic Sea since undersea cables represent a vital component for the national and collective security of the European Allies.

*The governance of the Baltic seabed*

The Baltic and North Seas present unique challenges to undersea cable governance due to their geographical and political realities, including maritime borders and the continental shelf. Although UNCLOS represented a leap forward in international cable governance, its signatories are nation-states. However, private companies from different nations build, own, and operate submarine cable networks, often grouped in international business consortiums. This poses challenges to their jurisdiction and for the protection of cables.

For instance, CITIC Telecom International, a Chinese-based company, owns the Baltic Sea Submarine Cable landing in Tallinn, Helsinki, and Stockholm, for a total length of 1042 km, while the supplier is Alcatel Submarine Networks (ASN), a Nokia company (TeleGeography, 2024). Beyond ASN, major suppliers for telecommunication cables worldwide include Prysmian Group (Italy-based), NEC (Japan), Huawei Marine Networks, another Chinese-based company, and SubCom (United States) (Bueger et al., 2022). Furthermore, tech giants such as Microsoft and Meta, among others, have recently financed and built their undersea cable networks (Bueger et al., 2022). This muddles the jurisdiction over telecommunication cables, which have always displayed an intrinsic dual-use nature. Indeed, alongside civilian digital consumption, these cables are necessary for diplomatic purposes, military communications, and intelligence collection (Bueger et al., 2022; Sunak, 2017).

Matters become even more complicated when the geography of the Baltic Sea is under consideration. All undersea cables and submarine infrastructure, in general, reside within the EEZs of the coastal countries. Nevertheless, the ownership, protection and governance outside the territorial seas remain subject to the established provisions of international law since considerations over the traditional 200-mile EEZs cannot apply to the Baltic Sea due to its small area with overlapping control and claims. This has noteworthy implications for the geopolitical environment.

Most Baltic Sea coastal states have now joined NATO. Denmark and Germany were the earliest Western powers to be present, with Copenhagen being a founding member of NATO and West Germany joining the Alliance in 1955 (Bruns, 2023). Estonia, Latvia, and Lithuania represent the continuation of the post-Cold War expansion as the Baltic republics gained accession in 2004, following in the footsteps of the Poles in 1999 (Westgaard, 2023; Bruns, 2023). More recently, the traditionally 'neutral' countries of Finland and Sweden abandoned their long-standing non-alignment policy to join NATO in 2023 and 2024, respectively, in the aftermath of Russia's full-scale invasion of Ukraine in 2022 (Bruns, 2023). Despite being an enclosed sea, the Baltic is governed and regulated as an open sea where access and naval activity are only limited by the maritime geography of the region, namely a small expanse and shallow waters (Engström, 2018). The Kiel Canal and the Baltic Sea, thus, represent key international bodies of water for trade, tourism, and naval exercises. In full compliance with international law, Russia possesses the right to use the Baltic and North Seas for commercial and military ventures despite the concerns about NATO's northern flank (Bruns, 2023). It is evident that the inadequacy of the established legal framework and the political geography of the Baltic region foster an ideal environment for damage to telecommunication cables due to the heavy traffic and for Russian hybrid actions against the European Allies.

## 2. The vulnerability of undersea cables: threats and risks

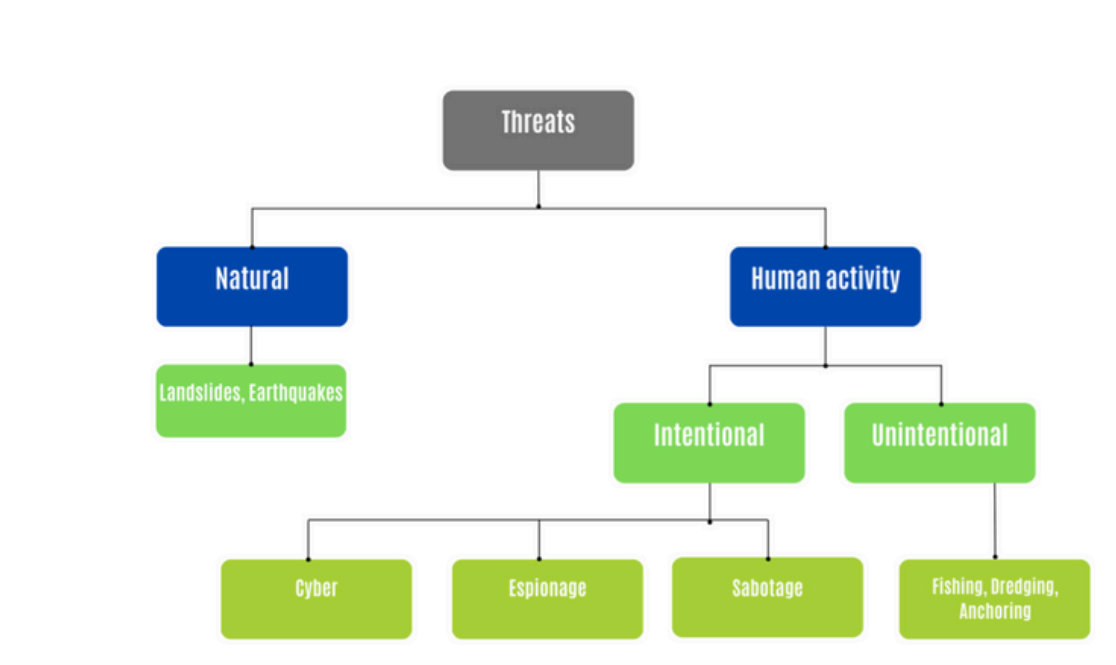


**Figure 1:** Threats to undersea telecommunication cables. Table created by the author building upon the literature.

Nowadays, sub-sea telecommunication cables are designed to be incredibly reliable according to the 'five nines' engineering standard reserved for nuclear weapons and space shuttles, i.e., they are built to be reliable 99,999% of the time (Sunak, 2017). Despite the structural reliability of the technology, undersea cables remain extremely vulnerable to various threats, and the infrastructure suffers from an estimated 100 to 150 cable ruptures per year (Bueger et al., 2022; Sunak, 2017; Chataut, 2024). Natural events and human activity represent the two primary threats to the integrity of the cable infrastructure (Figure 1). Since cables are privately owned and operated, the businesses that run the infrastructure are responsible for the maintenance and repair in the aftermath of these incidents (Sunak, 2017). Thus, mitigating threats to submarine telecommunication cables gives rise to an intertwined dynamic between the private companies and the state(s).

Indeed, the vulnerability of telecommunication cables underlines the strategic importance of maintaining connectivity and information networks, making countries exceptionally reliant on infrastructure resiliency and redundancy capacities (Bateman, 2024). Despite relatively frequent cable damage due to fishing activity, accidental ruptures pose a limited threat to European connectivity. For instance, the United Kingdom is linked to mainland Europe and the United States through over 30 fibre-optic cables, which underscores the robustness of its infrastructure (Sunak, 2017). Even if one or two cables suffer ruptures from unintentional

human activities such as fishing, dredging, or anchoring, sufficient spare capacity exists to reroute digital traffic with no interruption. Nonetheless, the danger of accidental cable outages has severe consequences in situations where cable capacity is limited. For example, in July 2017, Somalia experienced an almost complete internet blackout lasting three weeks due to damage to offshore cables; this incident, estimated to have incurred losses of approximately $10 million per day, amounted to roughly half of Somalia's daily national economic output (Sunak, 2017).

Accordingly, the interconnected nature of cable networks implies that global connectivity is affected by the complex interplay between geopolitical hotspots and infrastructure security (Chataut, 2024). Accidental cable disruptions in one area can significantly affect the economy or strategic communications of countries in different regions. For example, the unintentional severance by shipping traffic of three major undersea cables between Italy and Egypt in 2008 halted around 80% of the communication links from the Middle East to Europe and vice versa (Sunak, 2017). This incident had severe consequences for the operational capacity of the 200,000-strong American and British forces in Iraq due to the US government's reliance on commercial cables for military communications (Sunak, 2017). The US Air Force was particularly affected, with a sudden halt to their ability to conduct

Unmanned Aerial Vehicles (UAVs) combat missions (Sunak, 2017). More recently, in February 2024, communication networks in the Middle East suffered a major collapse when three undersea cables were cut in the Red Sea by the anchor of the sinking cargo vessel Rubymar due to a Houthis missile hit (Monaghan et al., 2024). This underscores the strategic importance of cable infrastructure worldwide.

Besides threats stemming from unintentional human activity, the paper considers the potential risks to telecommunication cable networks from deliberate actions of governments or non-state actors. On this, it is helpful to recall the incident that occurred in March 2013 off the coast of Alexandria, where three scuba divers were arrested by the Egyptian Navy while attempting to cut SeaWeMe-4, a 20,000-km long cable with the capacity to carry a third of the total telecommunication traffic between Europe and Egypt (Arthur, 2013). Egyptian authorities never released further details, including the motives. However, the incident emphasises the relatively low degree of sophistication necessary for sabotaging critical undersea infrastructure. Even actors with limited financial and conventional military resources could develop or acquire the capabilities to inflict severe damage to entire states and societies (Sunak, 2017). The effectiveness and the availability of 'sea drones' in the Russo-Ukrainian war since 2022 is a case in point where a dominant force––the Russian Black Sea fleet––suffered catastrophic damages to a much weaker adversary (Pili, 2024). Nevertheless, this paper is not concerned with the threats to undersea cables arising from

non-state or private actors.

Moving closer, the Baltic and North Seas have witnessed a sharp increase in critical undersea infrastructure incidents (Bashfield, 2024). Beyond Nord Stream 1 and 2, on October 8th, 2023, a natural gas pipeline named Balticconnectorand three undersea cables between Finland, Estonia, and Sweden were severed in a few hours. The Honk Kong-flagged container ship Newnew Polar Bear has been accused of sabotage by dragging its anchor (Braw, 2023; Bashfield, 2024; Kalm, 2024). Similarly, Norway's seabed telecommunications cables suffered alleged intentional physical damages in 2021 and 2022, posing a strategic threat to the country's scientific and economic interests and intelligence-gathering capabilities (Bashfield, 2024; Detsch and Johnson, 2024). The described incidents, likely stemming from deliberate actions of governments, bring us to the wider geopolitical confrontation between Moscow and NATO. In this context, Russia, as an adversary, stands out for its investment in seabed warfare.

Before moving to an in-depth analysis of Russian hybrid and seabed warfare capacity, the focus of this paper, cyber and network attacks, needs to be included in the present discussion. Protecting the infrastructure from cyber threats is a crucial task due to the ambiguity of the legislation and the relative lack of awareness about cyber-attacks (NATO CCDCOE, 2019). Thus, cyber and network attacks prove attractive to potential aggressors as they offer the advantage of plausible deniability (Canfil, 2022). Indeed, so far, the only documented case of a cyber-attack on submarine cable infrastructure occurred in April 2022, when the US Department of Homeland Security successfully disrupted an attack on the servers of an unnamed company responsible for the undersea cable in Hawaii (Vicens, 2022). Nevertheless, over the past few years, Chinese operations in cyberspace have expanded alongside the well-known capabilities of Russian actors (Siman, 2022). Therefore, cyber operations against critical (seabed) infrastructure will intensify as they represent an essential tool for conducting hybrid warfare (Siman, 2022).

## 3. The Nordic-Baltic Theatre: Hybrid and Seabed Warfare

Within the wider Baltic region, Russian sub-sea military capabilities stand out as a severe threat to the Allies' eastern and northern flanks. Since the end of the Cold War, the Kremlin has invested significant resources to build up its asymmetric seabed warfare capacities to threaten European critical infrastructure (Detsch & Johnson, 2024; Kaushal, 2023). The ability to target key enemy maritime assets is part of a broader Russian strategy to manage escalation and ensure deterrence (Kaushal, 2023). In other words, inflicting damages to critical infrastructure at sea and on land, like telecommunications and power cables, would allow Russia to contain conflicts within its periphery and undermine the popular support and

cohesion of the adversary (Kaushal, 2023). Indeed, under Russian military planning, the concept of 'strategic operations for the destruction of critically important targets', usually referred to as SOPKVO or SODCIT, has rightly received close attention from Allied nations (Kofman et al., 2021). This concept entails the infliction of material and psychological damage to the adversary by attacking crucial targets with economic-military and political significance to manage escalation beneficial to Moscow (Kofman et al., 2021). The main assumption underpinning the choice of targets is that the opponent's economic and military system depends on key nodes which sustain the military potential of the enemy state (Kofman et al., 2021). By destroying these systemic keystones, Russia can lower the military-economic capacity of the adversary and produce an exponential psychological impact on the leaders' will to fight (Kofman et al., 2021).

Thus, Western social, political, economic, and military systems heavily rely on the continuous and widespread operations of the telecommunication infrastructure lying beneath the oceans (Solarz Hendriks & Halem, 2024). Against this backdrop, the seabed has emerged as a crucial space for confrontation between Russia and NATO. The inherent characteristics of the seabed, i.e., its size and inaccessibility, make it an ideal environment for hybrid warfare as dual-use technologies increasingly undermine the existing legal maritime framework (Solarz Hendriks & Halem, 2024). In the last two decades, the Kremlin has sought to transition from a purely conventional maritime power primarily focused on surface naval forces to an expansion of its sub-surface military domain (Solarz Hendriks & Halem, 2024). The overarching strategic aim is to acquire the asymmetric capacity to wage hybrid warfare while firmly remaining below the threshold of war with NATO countries (Kofman et al., 2021). Relevantly, Moscow's ability to rapidly degrade Kyiv's internet infrastructure during the invasion of Crimea in 2014 clearly illustrates the Russian doctrine of hybrid war (Solarz Hendriks & Halem, 2024). In the Nordic-Baltic theatre, the disruption to undersea telecommunication cables, combined with disinformation campaigns and more traditional military threats, have the potential to incapacitate Western societies and states, thereby achieving a strategic advantage (Solarz Hendriks & Halem, 2024). Indeed, in the aftermath of the disintegration of the Soviet Union, Russia has long since lacked the conventional warfighting capabilities to upset the security architecture of Europe's eastern flank thus, asymmetric methods and hybrid warfare provide the Kremlin with a strategic advantage coherent with the overarching 'offensive defence' thinking of Russian military planners (Kofman et al., 2021; Solarz Hendriks & Halem, 2024). For Moscow, the Baltic region represents both a security challenge and the 'decisive point' to weaken NATO, borrowing from Baron de Jomini's military lexicon (Solarz Hendriks & Halem, 2024). Russian military theorists acknowledge the technological and economic disadvantage that the country needs to overcome in a long-term confrontation with the West. This rationale of Russia as the weaker power entirely drives the Kremlin's objective to inflict greater relative costs on the

opponents. This makes the North and Baltic Seas crucial pressure points due to the vital role they play for Allied communications and economies whilst being strategically vulnerable (Solarz Hendriks & Halem, 2024). This would force NATO powers to react overwhelmingly to any type of disruptive threats in the theatre.

*Russian military capabilities in the Nordic-Baltic Theatre*

Seabed warfare is, therefore, a core tenet of Russian naval doctrine and force structure. The responsibility for special operations in this realm is assigned to the Navy and the Main Directorate for Deep Sea Research, or GUGI (Kaushal, 2023). Whilst the Russian Navy retains a key operational role, ultimate control is exerted by the Ministry of Defence (MoD) and the GRU via the Intelligence Directorate of the Russian Naval Staff and the GUGI, which is organisationally independent from the naval command as a per se directorate of the MoD (Kaushal, 2023).

The GUGI, founded in 1965, operates a special-purpose fleet and is supported by the 29th Separate Submarine Division from the naval base of Olenya Guba (Trakimavičius, 2021; Kaushal, 2023). The GUGI operates nuclear-powered special mission submarines such as the Paltus, X-Ray, Kashalot and Losharik, which are all built for operations at extreme depths, alongside larger 'motherships' like the Belgorod (Kaushal, 2023). Moreover, intelligence-gathering, or 'oceanographic,' surface ships like the Yantar are employed for unconventional missions since they are usually equipped with deep-diving crewed submersibles and unmanned submarine vehicles with operational depths well over 6,000 meters below the waters (Sutton, 2021; Trakimavičius, 2021; Kaushal, 2023). Besides the GUGI, the Russian Navy's Intelligence Directorate, which is closely intertwined with the GRU, has been recognised as an essential player in the field. Relevantly for the scope of this article, the special mission ship Akademik Vladimirsky, belonging to the Baltic fleet, has been spotted in the vicinity of key undersea infrastructure in the region (Kaushal, 2023).

*NATO's tools to counter Russian threats*

The equilibrium between offence and defence tends to shift rapidly on traditional battlefields. However, in seabed warfare, the aggressors currently hold a major advantage partly due to the sheer scale of the infrastructure to defend and the complexity of the operational space (Kington, 2024). This is not a novel perception (Detsch & Johnson, 2024). Since the late 1950s, the hovering and activity of Soviet vessels near strategic undersea cables across the Atlantic have drawn the attention of Western intelligence communities, although with no conclusive outcome (Bateman, 2024). However, as space telecommunications technologies developed in the following decades, making Allied

communications more resilient, undersea telecommunications networks became largely invisible (Bateman, 2024). Combined with Western disinvestment in anti-submarine warfare following the end of the Cold War, the vulnerability of undersea infrastructure is an immediate threat to the security of NATO European Allies who have been largely unprepared to counter Russian hybrid interference with critical submarine cables (Solarz Hendriks & Halem, 2024). Nevertheless, NATO likely remains the sole actor with the capability to deter aggressors and protect undersea telecommunication infrastructure in the Nordic and Baltic regions (Monaghan et al., 2023).

Indeed, in 2023, the Critical Undersea Infrastructure Coordination Cell (CUICC) was established in Brussels by NATO (Solarz Hendriks & Halem, 2024; NATO, 2023). This joins the Maritime Centre for the Security of Critical Underwater Infrastructure, established at Allied Maritime Command (MARCOM) in the aftermath of the 2023 Vilnius Summit (Monaghan et al., 2023). These initiatives aim to create an efficient alert system to respond to any disruption to the cable networks by bringing together the relevant private companies and national officials at MARCOM (Detsch & Johnson, 2024). Similarly, NATO allies facing the Baltic and North Seas have recently begun sharing the necessary information to jointly protect sub-sea infrastructure. The proactive efforts of the Alliance's member states complement NATO's reactive approach to seabed threats (Detsch & Johnson, 2024). France released its own Seabed Warfare Strategy in 2021 and, more recently, Italy has set up the National Sub-Sea Hub in La Spezia under the naval command (Solarz Hendriks & Halem, 2024; Detsch & Johnson, 2024). Beyond purely national ventures, within the NATO framework, the 10-nation Joint Expeditionary Force (JEF), led by the United Kingdom, is dedicated to the protection of critical undersea infrastructure in the AoR––the Nordic-Baltic region (Solarz Hendriks & Halem, 2024; Detsch & Johnson, 2024). Despite the limitations and the early unpreparedness, the Alliance is rapidly adapting its forces and strategic vision to an era of contestation on the seabed in the North and Baltic Seas.

**Conclusion**

Seabed warfare is rapidly gaining prominence within the wider geopolitical confrontation between Russia and NATO European allies. The telecommunications cables, and the infrastructure in general, lying beneath the waters of the Baltic and North Seas, which have a vital economic, informational, and military importance, are exposed to increasing Russian hybrid threats. Incidents in the Nordic-Baltic region involving the suspicious ruptures of undersea cables underline the vulnerability of this critical infrastructure and the inability of NATO allies to effectively counter and deter aggressors in the grey zone. This paints a worrisome picture considering the extensive seabed military capabilities and the hybrid warfare doctrine of the Russian Federation. With degraded conventional forces after more

than two years of high-intensity warfare in Ukraine, the Kremlin may seek to increasingly target critical telecommunications infrastructure within its reach in the Baltic-Nordic region to exponentially impact European security as part of an asymmetric strategy. But more than military threats, undersea cable insecurity is compounded by an ill-equipped international legal architecture which seems inadequate for the protection of sub-sea cables within the tense political geography of the wider Baltic region. Further, the intricate interplay between private governance and the geopolitical weight of the infrastructure puts European Allies at a disadvantage regarding safeguarding and protecting undersea cables. As the seabed domain is increasingly accessible to malicious actors for highly disruptive actions, the European Allies need to develop the necessary submarine and surface maritime capabilities to counter the hybrid threats to their undersea infrastructure.

**Bibliography**

Arthur, C. (2013, March 28). Undersea internet cables off Egypt disrupted as navy arrests three. The Guardian. https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests

Australian Government. (2024). Protection zone for Sydney submarine cable. ACMA. https://www.acma.gov.au/zone-protect-sydney-submarine-cables

Bashfield, S. (2024). Defending seabed lines of communication. Australian Journal of Maritime & Ocean Affairs, 1–13. https://doi.org/10.1080/18366503.2024.2363607

Bateman, A. (2024). The weakest link: The vulnerability of U.S. and allied global information networks in the nuclear age. Journal of Strategic Studies, 1–30. https://doi.org/10.1080/01402390.2024.2360724

Bearn, L. & Bentham, J. (2024). Europe's critical-maritime-infrastructure protection: still in the pipeline? IISS. https://www.iiss.org/online-analysis/military-balance/2024/09/europes-critical-maritime-infrastructure-protection-still-in-the-pipeline/

Bergeron, J. H. (2023, February 17). Reflecting on One Year of War: A Transformational Year in Maritime NATO. Center for Maritime Strategy. https://centerformaritimestrategy.org/publications/reflecting-on-one-year-of-war-a-transformational-year-in-maritime-nato/

Braw, E. (2023, October 24). Baltic Sea Saboteurs Strike Again. CEPA. https://cepa.org/article/baltic-sea-saboteurs-strike-again/

Bruns, S. (2023). From "Flooded Meadow" to Maritime Hotspot: Keeping the Baltic Sea Free, Open, and Interconnected. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/from-flooded-meadow-to-maritime-hotspot-keeping-the-baltic-sea-free-open-and-interconnected?lang=en

Bueger, C., Liebetrau, T. & Franken, J. (2022). Security threats to undersea communications cables and infrastructure consequences for the EU. European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Canfil, J. K. (2022). The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay. Journal of Cybersecurity, 8(1). https://doi.org/10.1093/cybsec/tyac007

Chataut, R. (2024, April 1). Undersea cables are the unseen backbone of the global internet. The Conversation. https://theconversation.com/undersea-cables-are-the-unseen-backbone-of-the-global-internet-226300

Convention for the Protection of Submarine Telegraph Cables, March 14, 1884. https://www.iscpc.org/documents/?id=13

Convention on the High Seas, April 29, 1958.

Detsch, J. & Johnson, K. (2024, June 28). NATO Wants to Boost Its Undersea Defenses. Foreign Policy. https://foreignpolicy.com/2024/06/24/nato-undersea-cable-network-russia-infrastructure-defense/

Engström, V. (2018). Complexities of the Baltic Sea regulatory framework. Marine Policy, 98, 191–200. https://doi.org/10.1016/j.marpol.2018.09.014

Galeotti, M. (2023, April 20). Russia's spy ships are playing mind games in British waters. The Spectator. https://www.spectator.co.uk/article/russias-spy-ships-are-playing-mind-games-in-british-waters/

Kalm, H. (2024). NATO's Path to Securing Undersea Infrastructure in the Baltic Sea. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/05/nato-baltic-sea-security-nord-stream-balticconnector?lang=en¢er=india

Kaushal, S. (2023). Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure. RUSI. https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure

Kington, T. (2024, January 4). European navies try to keep up in cat-and-mouse game of seabed warfare. Defense News; Defense News. https://www.defensenews.com/global/europe/2024/01/04/european-navies-try-to-keep-up-in-cat-and-mouse-game-of-seabed-warfare/

Kofman, M., Fink, A., Gorenburg, D., Chesnut, M., Waller, J., Stricklin, K. & Bendett, S. (2021). Russian Military Strategy: Core Tenets and Operational Concepts. CNA. https://www.cna.org/reports/2021/08/Russian-Military-Strategy-Core-Tenets-and-Operational-Concepts.pdf

Monaghan, S., Darrah, M., Jakobsen, E. & Svendsen, O. (2024). Red Sea Cable Damage Reveals Soft Underbelly of Global Economy. Center for Strategic and International Studies. https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy

Monaghan, S., Svendsen, O., Darrah, M. & Arnold, E. (2023). NATO's Role in Protecting Critical Undersea Infrastructure. Center for Strategic and International Studies. https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure

NATO. (2023, February 15). NATO Stands up Undersea Infrastructure Coordination Cell. NATO. https://www.nato.int/cps/en/natohq/news_211919.htm

NATO CCDCOE. (2019). Strategic importance of, and dependence on, undersea cables. NATO CCDCOE. https://www.ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf

Pili, G. (2024, September 5). Sea drones at war: Tactical, operational and strategic analysis of maritime uncrewed systems. European Security & Defence. https://euro-sd.com/2024/09/articles/40191/sea-drones-at-war-tactical-operational-and-strategic-analysis-of-maritime-uncrewed-systems/

Siman, B. (2022). Hybrid Warfare Is Not Synonymous with Cyber: The Threat of Influence Operations. Egmont Institute. https://www.egmontinstitute.be/app/uploads/2022/02/spb155-siman-final-version_0222.pdf?type=pdf

Solarz Hendriks, M. & Halem, H. (2024). From space to seabed. Protecting the UK's undersea cables from hostile actors. Policy Exchange. https://policyexchange.org.uk/wp-content/uploads/From-space-to-seabed.pdf

Sunak, R. (2017). Undersea Cables Indispensable, insecure. Policy Exchange.

Sutton, H. I. (2021, August 19). Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables. Naval News. https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/

TeleGeography. (2024). Submarine Cable Map. Submarinecablemap.com. https://www.submarinecablemap.com/submarine-cable/baltic-sea-submarine-cable

The Upfront Team. (2023, November 10). Why are subsea cables off Ireland causing continental concerns? RTE. https://www.rte.ie/news/upfront/2023/1110/1415821-why-are-subsea-cables-off-ireland-causing-continental-concerns/

Trakimavičius, L. (2021). The Hidden Threat to Baltic Undersea Power Cables. NATO Energy Security Centre of Excellence. https://www.enseccoe.org/wp-content/uploads/2024/01/2021-12-the-hidden-threat-to-baltic-undersea-power-cables-final.pdf

Westgaard, K. (2023). The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en