Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Research Article

PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE AND STRENGTHENING BALTIC SEA SECURITY: NATO'S OPERATION BALTIC SENTRY

English translation with AI assistance (DeepL)

Mónica Román González
PhD Candidate in the Political Science and Administration and International Relations Programme at the Complutense University of Madrid.
Master in International Politics: sectorial and area studies at the Complutense University of Madrid.
monicaromangz@gmail.com
ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Received 31/03/2025
Accepted 28/05/2025
Published 27/06/2025

Recommended citation: Román, M. (2025). The protection of critical underwater infrastructures and the strengthening of Baltic Sea security: NATO's Baltic Sentry operation. *Revista Logos Guardia Civil*, 3(2), p.p. 221-256.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE AND STRENGTHENING BALTIC SEA SECURITY: NATO'S OPERATION BALTIC SENTRY

Abstract: Damage to undersea cables in the Baltic Sea has raised alarms about the potential for hybrid warfare and the vulnerability of Western critical undersea infrastructures to sabotage, with repeated incidents in this area being one of the main examples of the geopolitical tensions that exist today. The main objective of this article is to analyse NATO's Operation *Baltic Sentry* in the context of the Atlantic Alliance's growing need to ensure the protection of this type of critical infrastructure in the strategic Baltic Sea and thus reinforce security over the latter. Using mixed research methods, this article first explains the importance of protecting critical undersea infrastructure in the geostrategically important Baltic Sea and then outlines NATO's general framework for protecting such infrastructure. The study then sets out the main characteristics of Operation *Baltic Sentry* launched by NATO in January 2025, concluding that it meets the needs required to be a good strategy capable of enabling the Alliance to make progress in achieving two of its main priority objectives: the protection of increasingly important infrastructures such as critical undersea infrastructures and the consequent reinforcement of security in the Baltic Sea in order to guarantee its resilience.

Resumen: Los daños sobre los cables submarinos en el Mar Báltico han encendido las alarmas sobre una potencial guerra híbrida y la vulnerabilidad de las infraestructuras críticas submarinas occidentales ante posibles sabotajes, siendo así los reiterados incidentes sobre la zona señalada uno de los principales ejemplos de las tensiones geopolíticas existentes en la actualidad. El presente artículo tiene como principal objetivo analizar la Operación *Baltic Sentry* de la OTAN en un contexto en el que impera la creciente necesidad de la Alianza Atlántica de asegurar la protección de este tipo de infraestructuras críticas en el estratégico Mar Báltico y de reforzar así la seguridad sobre este último. Para ello, a través del empleo de métodos mixtos de investigación, el presente artículo primero explica la importancia de la protección de infraestructuras críticas submarinas en una zona de gran relevancia geoestratégica como es el mencionado Mar Báltico para después exponer el marco general de acción de la OTAN respecto a la protección de estas infraestructuras. Tras ello, el estudio expone las principales características de la Operación *Baltic Sentry* lanzada por la OTAN en enero de 2025 concluyendo que esta se ajusta a las necesidades requeridas para ser una buena estrategia capaz de permitir a la Alianza avanzar en la consecución de dos de sus principales objetivos prioritarios: la protección de unas infraestructuras cuya importancia es cada vez mayor como son las infraestructuras críticas submarinas y el consiguiente refuerzo de la seguridad en el Mar Báltico en pro de garantizar su resiliencia.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Keywords: North Atlantic Treaty Organisation (NATO), Baltic Sea, critical undersea infrastructure, security, Baltic Sentry.

Palabras clave: Organización del Tratado del Atlántico Norte (OTAN), Mar Báltico, infraestructuras críticas submarinas, seguridad, Baltic Sentry.

ABBREVIATIONS

CCD COE: Cooperative *Cyber Defence Centre of Excellence*

CCOE: Civil-Military *Cooperation Centre of Excellence*

CMRE: NATO *Centre for Maritime Research and Experimentation*

CONVEMAR: United Nations Convention on the Law of the Sea

RRC: Resilience *Reference Curriculum*

CTF: *Commander Task Force* Commander

LNG: Liquefied Natural Gas

GUGI: *Glavnoye upravlenie glubokovodnikh issledovanii* or Main Directorate for Deep-sea Research

MARCOM: *Allied Maritime Command* or NATO Naval Command *UK*

NATO: *North Atlantic Treaty Organisation*

NSC: *NATO Shipping* Centre

NATO: North Atlantic Treaty Organisation

SOFCOM: Allied *Special Operations Forces Command*

EU: European Union

USSR: Union of Soviet Socialist Republics

USV: Unmanned *Surface Vehicle*

EEZ: Exclusive Economic Zone

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

1. INTRODUCTION

In recent times, the importance of critical undersea infrastructures has increased dramatically as they facilitate the provision of basic services such as energy, financial transactions, communications or the Internet. This makes the vulnerability of these infrastructures a major concern for international actors, especially given that control of the seabed continues to emerge as a determining element in the power relations of this century (Conte de los Ríos, 2025, p. 34). While the recent proliferation of undersea technology and the consequent acquisition of the capacity to conduct sophisticated operations have favoured their protection capabilities, such innovations also offer a range of possibilities to those actors who wish to exploit their weaknesses (Cassetta, 2024, p. 2).

In this sense, any attack against the North Atlantic Organisation's (NATO) submarine infrastructure would have serious consequences for the security of its member states, making it a target for its rivals. Bearing in mind that an attack on these cables requires the availability of precise means, Russia and to a lesser extent China are the countries that could be identified as the most direct threat, according to the Insikt Group (2023, p. 11-15) in its latest report on the risks to submarine cables.

Thus, the so-called "seabed *warfare*", more commonly known as *Seabed Warfare*, is now an immediate threat to the Atlantic Alliance. Episodes such as the repeated incidents involving submarine cables in the geostrategic Baltic Sea highlight the magnitude of the risks posed by a threat that requires coordinated efforts and investments to complement the strategies designed by each state. This is where NATO's new operation to protect critical undersea infrastructure in the Baltic Sea - Operation *Baltic Sentry* - comes into play.

There is a wide range of literature on this issue. On the one hand, the main reasons that explain the importance of protecting critical underwater infrastructures are widely covered in research by experts in the field such as Noelia Arjona Hernández (2023), Rafael García Pérez (2024) and Augusto Conte de los Ríos (2025). On the other hand, regarding NATO's role in protecting these infrastructures, the report by Njall Trausti Fridbertsson (2023) or the article by Sean Monaghan, Otto Svendsen, Michael Darrah, and Ed Arnold for the *Center for Strategic & International Studies* (2023) are noteworthy. In light of this, the overall objective of this study is to analyse the recently announced Operation *Baltic Sentry* within NATO's framework for strengthening Baltic Sea security through the protection of critical undersea infrastructure.

Accordingly, the overall research question guiding this study is: How does NATO's Operation *Baltic Sentry* respond to the protection of critical undersea infrastructure in the Baltic Sea? The general hypothesis of the research is that Operation *Baltic Sentry* enhances the protection of critical undersea infrastructure in the Baltic Sea and the Alliance's presence in the Baltic Sea, thus adjusting to the new threat environment.

To this end, two specific objectives have been defined. First, to explain the importance of protecting critical undersea infrastructures in an area of great geostrategic relevance such as the Baltic Sea, especially in the current international context marked by the Russian threat following its invasion of Ukraine and the increase in damage suffered by this type of infrastructure since then. Second, to set out NATO's general framework for action with respect to the protection of critical undersea infrastructures.

Thus, having used mixed research methods, the study concludes with conclusions regarding NATO's new project as it attempts to address two increasingly important security issues: the protection of critical undersea infrastructures and the consequent strengthening of Baltic Sea security.

2. FRAMEWORK OF THE STUDY

2.1. THE GEOSTRATEGIC IMPORTANCE OF THE BALTIC SEA

Located in northern Europe (see Figure 1), the Baltic Sea has historically been an area of geopolitical competition, which has now re-emerged as a crucial point of threat to European security following the invasion of Ukraine. Beyond its commercial and marine resource benefits, this enclave is a key hub for infrastructures that contribute significantly to the energy supply of several European states, themselves NATO members (Fridbertsson, 2023, p. 2).

The Alliance itself defines it as "a vital hub for trade and energy transport connecting numerous allied nations" by being a conduit for both energy supplies and a support for undersea cables that transfer data, two crucial elements for the Allied economy and security (NATO Allied Maritime Command, 2025a).

Figure 1

Political map of the Baltic Sea.

Source: McNamara (2016).

With Finland and Sweden joining NATO in 2023 and 2024, the Baltic Sea has become known as 'NATO's Lake'. However, this label is not adequate enough considering that the Allies in the region still face numerous threats and, as defined by John Deni (2023), a dynamic regional security landscape that forces them to join forces through the different cooperation frameworks at their disposal. This situation stems mainly from Russia's presence in the region, which poses increasing challenges to Allied security,

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

especially in the current context that makes the protection of NATO's so-called eastern flank a priority security issue.

Historically, Russia has been a major player in the Baltic region. On the one hand, it has the port city of St. Petersburg, an important economic and cultural centre of the country through which most of its maritime trade has passed since the time of Peter the Great. On the other, Russia also controls the Kaliningrad enclave between Poland and Lithuania, where it has military bases with the Baltic Fleet (Savitz and Winston, 2024, p. 5).

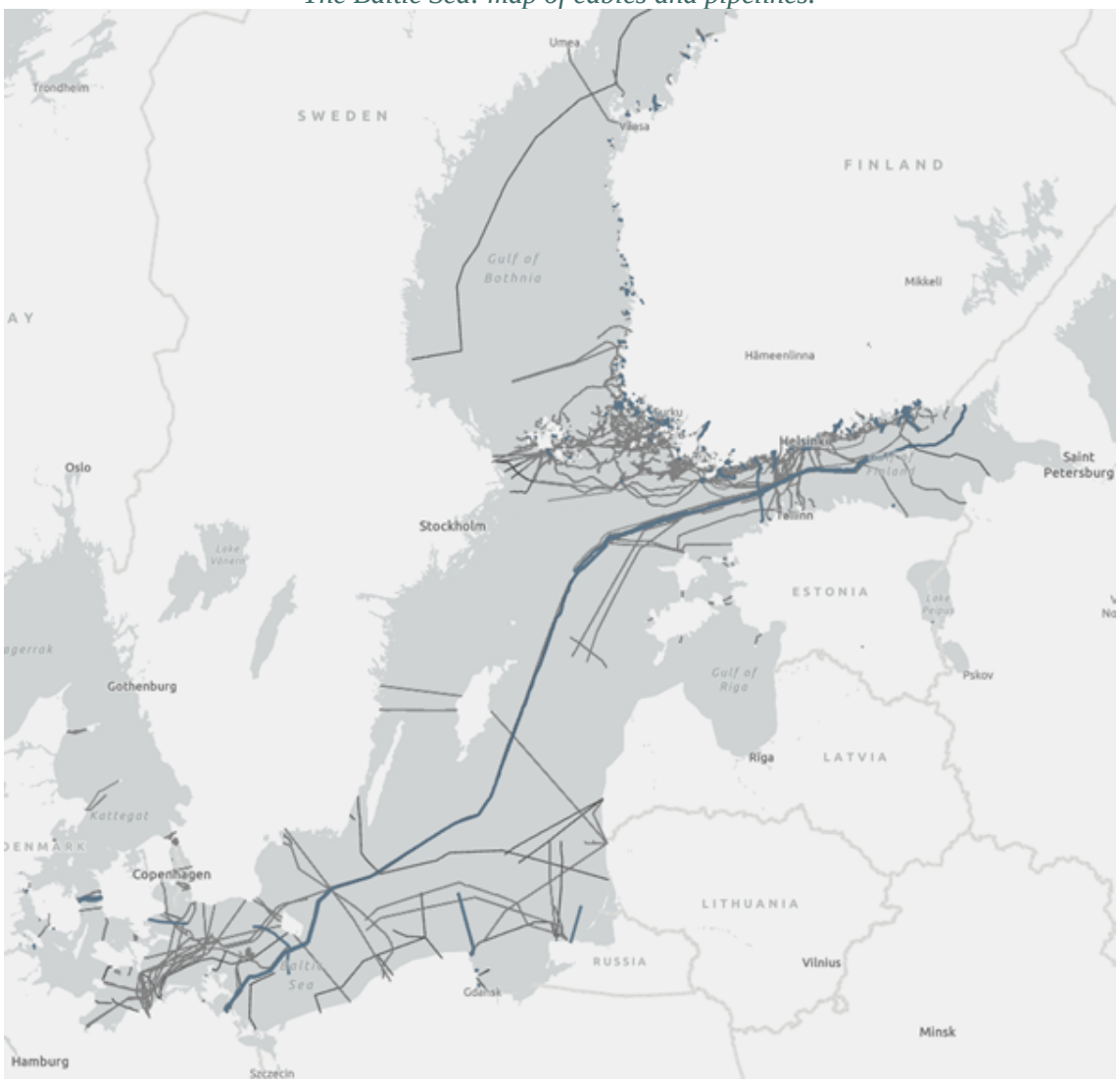
In addition, the so-called 'Russian Ghost Fleet', a Kremlin-created tanker fleet that sails under the flags of other nations in order to evade sanctions imposed after its illegal aggression against Ukraine, is currently operating in the Baltic Sea (Childs, 2025, p 5). Like other Russian vessels, this one is equipped with technology capable of monitoring the seabed and is therefore also suspected of participating in Russia's hybrid campaign against the West through intelligence gathering and the subsequent preparation of sabotage of critical undersea infrastructure (Jones, 2025, p 8). Added to this is the fact that Moscow has repeatedly demonstrated its expansionist ambitions over a region that could be its next target, especially at the height of its hostility towards NATO.

Consequently, Russia is the main challenge to the Alliance in the region. In the region, Moscow finds hybrid tactics to be the main tool for pressuring allies to mitigate conventional military weaknesses and minimise the risks of provoking a direct confrontation between the parties (Cassetta, 2024, p. 2). As is well known, sabotage is executed in a way that makes it difficult to identify those responsible, causing the countries concerned to be cautious in assigning responsibility for fear of escalation. Thus, they are useful to Russia in undermining NATO by preventing the activation of Article 5 collective defence (Jones, 2025, p. 3).

At the same time, it is worth noting that Russia's submarine capabilities are its main strength in competing in the region. As Sidharth Kaushal (2023) explains, Moscow has the Main Directorate for Deepwater Research (*Glavnoye upravlenie glubokovodnikh issledovanii*, GUGI), a secret agency under the Russian Ministry of Defence that operates submarines and vessels capable of engaging in sabotage.

Considering that Russia's critical infrastructure attack capabilities are a fundamental component of its strategy (Fink and Kofman, 2020, p. 16), they could be used to intercept critical communications in the Baltic region (Metrick and Hicks, 2018, p. 7). This region is home to a complex network of undersea infrastructure that is key to communication and energy supply between European nations (see Figure 2).

Figure 2
The Baltic Sea: map of cables and pipelines.



Source: Baltic Marine Environment Protection Commission (2024).

The protection of these critical maritime infrastructures in this key geostrategic region relies heavily on NATO (Fridbertsson, 2023, p. 11), which opens a window of opportunity for Moscow in its desire to weaken the West.

2.2. PROTECTION OF CRITICAL INFRASTRUCTURE UNDERWATER

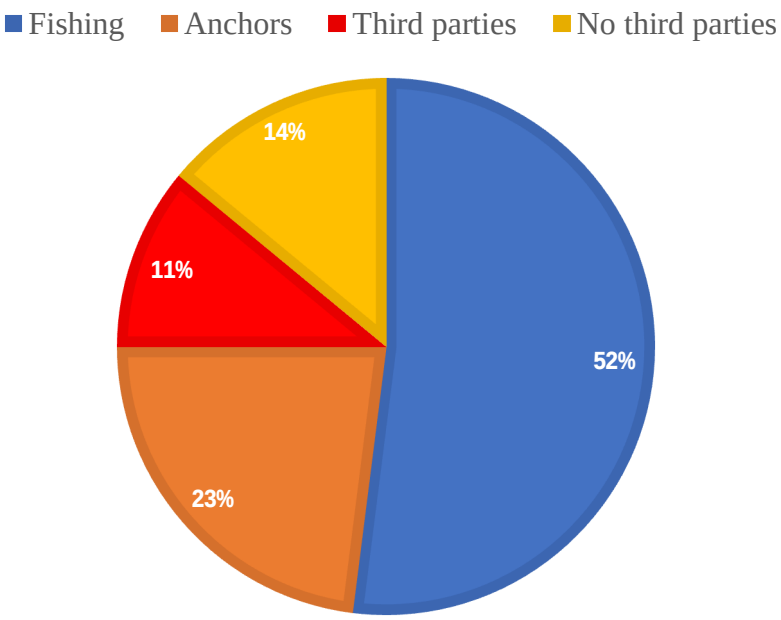
Communications, financial transactions, energy and a wide range of essential daily activities depend on critical undersea infrastructures. According to data provided by the *Submarine Telecoms Forum* (2025, p. 8-9) in its latest report, 99% of international data traffic transits through submarine cables, making them "the backbone of global communications".

Its importance is such that any damage to it can have serious consequences for the stability of society, which makes its security of key geostrategic importance, making it a priceless asset whose protection must be a priority in security agendas (Quijarro Santibáñez, 2023, p. 15-22) (Fridbertsson, 2023, p. 2) (García Pérez, 2024, p. 265-298).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

The increasing dependence on undersea critical infrastructure and the current convergence of traditional and emerging threats make their protection one of the greatest security challenges (Conte de los Ríos, 2025, p. 26), especially given their vulnerability to natural and man-made threats (Guilfoyle, Paige and McLaughlin, 2022, p. 657-696). The *International Cable Protection Committee* (2024, p. 5) argues that human interaction is the most common cause of damage to cables, generally caused by fishing and anchors (see Figure 3).

Figure 3
Chart of the main causes of cable breaks/breaks according to the International Cable Protection Committee.



Source: International Cable Protection Committee (2024, p. 5).

Already in 2016, in the face of increasing Russian submarine activity to an extent not known since the Cold War, James Foggo and Alarik Fritz (2016) proposed their idea of the existence of "The Fourth Battle of the Atlantic" in which undersea infrastructures, in particular energy supply platforms and telecommunications cables, would be threatened. A battle that, according to James Foggo (2023), began in earnest after the apparent attack on the Nord Stream pipeline in 2022.

The fact is that the importance of these infrastructures has made them not only a priority target for protection, but also a possible target for attacks by actors interested in destabilising others. Incidents such as the one mentioned above have raised awareness of the vulnerabilities of these infrastructures in the context of international tensions, which has led to a turning point in the understanding that the adoption of measures to guarantee their protection is fundamental (Fridbertsson, 2023, p. 11) (Monaghan et al., 2023, p. 2).

On the other hand, the constant technological evolution entails important repercussions in terms of the submarine capabilities that the different actors must acquire (Clark, 2015, p. 18), something that has significantly contributed to the consolidation of the submarine domain as the so-called "sixth domain". This new operational domain,

which is increasingly disputed, concentrates economic, strategic and military interests due to the wealth of resources it harbours and which make it a theatre of conflict known as *Seabed Warfare* (Conte de los Ríos, 2025, pp. 29-30). Although its conceptualisation is still being developed by actors such as NATO, Conte de los Ríos (2025, p. 29) defines it as the set of operations carried out in, to, from, on and under the seabed for strategic or military purposes, using the sabotage of the Nord Stream gas pipeline as a representative case.

The maritime domain is particularly vulnerable to hybrid threats. In addition to the fact that the latter are difficult to distinguish from accidental damage, aggressors may use the cover of vessels of various kinds that are difficult to track, such as fishing vessels or private vessels (Monaghan et al., 2023, p. 6). In this regard, it should be recalled that, as sabotage is not considered a violation of the prohibition of the use of force under the UN Charter, international law restricts the military response to damage to cables, especially when non-military vessels are involved (Conte de los Ríos, 2023, p. 33).

Christian Bueger and Tobias Liebetrau (2021) argue that the governance of underwater critical infrastructures is more complex due to two factors: (1) the need for international cooperation by various state actors -who act on the basis of their strategic benefits- and (2) the fact that part of these infrastructures are owned by the private sector -whose role is relevant considering that their interests may be misaligned with the interests of states-. This complexity makes it difficult to apply effective legal provisions in case of damage to critical underwater infrastructures (Conte de los Ríos, 2023, p. 32).

The legal regime applicable to submarine infrastructure is based on international instruments, among which the Convention for the Protection of Submarine Telegraph Cables of 1884 and the United Nations Convention on the Law of the Sea (UNCLOS) of 1982 stand out. The latter establishes that all states have the right to install submarine cables and pipelines on the continental shelf, in accordance with the national legislation of the coastal state concerned (Arjona Hernández, 2023, p. 48). Likewise, UNCLOS delimits different maritime spaces - territorial waters, Exclusive Economic Zones (EEZs) and the high seas - attributing full sovereignty in the former, limited rights in EEZs and a less well-defined regulatory framework in international waters, where the military activity of other states cannot be legally restricted (McNamara, 2024).

It should be noted that among the emerging challenges to international maritime law are Unmanned Underwater Vehicles (UUVs) and Unmanned Maritime Systems (MUS), whose legal status remains undefined. The absence of a specific regulatory framework for their international operation complicates their integration into current regimes, particularly with regard to UNCLOS (Conte de los Ríos, 2023, p. 32). In this context, the growing importance of critical underwater infrastructures makes it indispensable to advance towards an effective international legal framework that guarantees their protection (García Pérez, 2023, p. 50).

Given the importance of these infrastructures and their complex legislation, Michael McNamara (2024) explains that, as geopolitical tensions between the West and its competitors increase, these infrastructures are a target as hybrid interference is a useful tool in its aim to challenge the interests of Euro-Atlantic democracies. These currently face their main threat in Russia's hybrid actions (Monaghan et al., 2023, p. 2), particularly in the Baltic Sea where it has strengthened its presence by investing in submarine capabilities, considered its main asset (Gresh, 2023, pp. 3-4).

Taking into account the complex context and the situation of the Baltic Sea, experts such as Conte de los Ríos (2025), Njall Trausti Fridbertsson (2023) and Monaghan et al (2023) agree on a series of key elements for defining an effective protection strategy.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Recognising that it is essential to strengthen detection, deterrence-prevention, adaptation and response capabilities, the elements to be highlighted are: (1) increased presence or surveillance, (2) collaboration between actors, (3) coordination with the private sector, (4) advanced technology, (5) regulatory frameworks, (6) response measures and (7) renewing maritime strategies.

2.3. THE SITUATION OF CRITICAL UNDERWATER INFRASTRUCTURE IN THE BALTIC SEA SINCE THE START OF THE RUSSIAN FULL-SCALE INVASION OF UKRAINE IN 2022

On 26 September 2022, the Danish Maritime Authority reported several methane leaks caused by a series of underwater explosions off the Danish island of Bornholm that severely damaged the Nord Stream pipeline (see Figure 4), cutting off the supply of Russian gas to the European market via the Nord Stream pipeline (Energistyrelsen, 2022).

Figure 4

Map of the Nord Stream 1 and Nord Stream 2 pipelines next to the methane leaks detected in September 2022.

Source: The European Space Agency (2022).

Regardless of the unknown perpetrator of the apparent sabotage, experts agree that this was a turning point for the Allies to consider efforts to improve their ability to defend against hybrid tactics in the submarine domain (Monaghan, 2022) (Fridbertsson, 2023) (Conte de los Ríos, 2025).

A similar case was recorded in October 2023 with the Balticconnector pipeline incident. This infrastructure, together with the Inkoo liquefied natural gas (LNG) terminal, safeguards the security of supply and energy independence of the countries in the area (see Figure 5).

Figure 5

Map of the gas transmission network in Finland and the Baltic States.

Source: Gasgrid (n.d.)

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

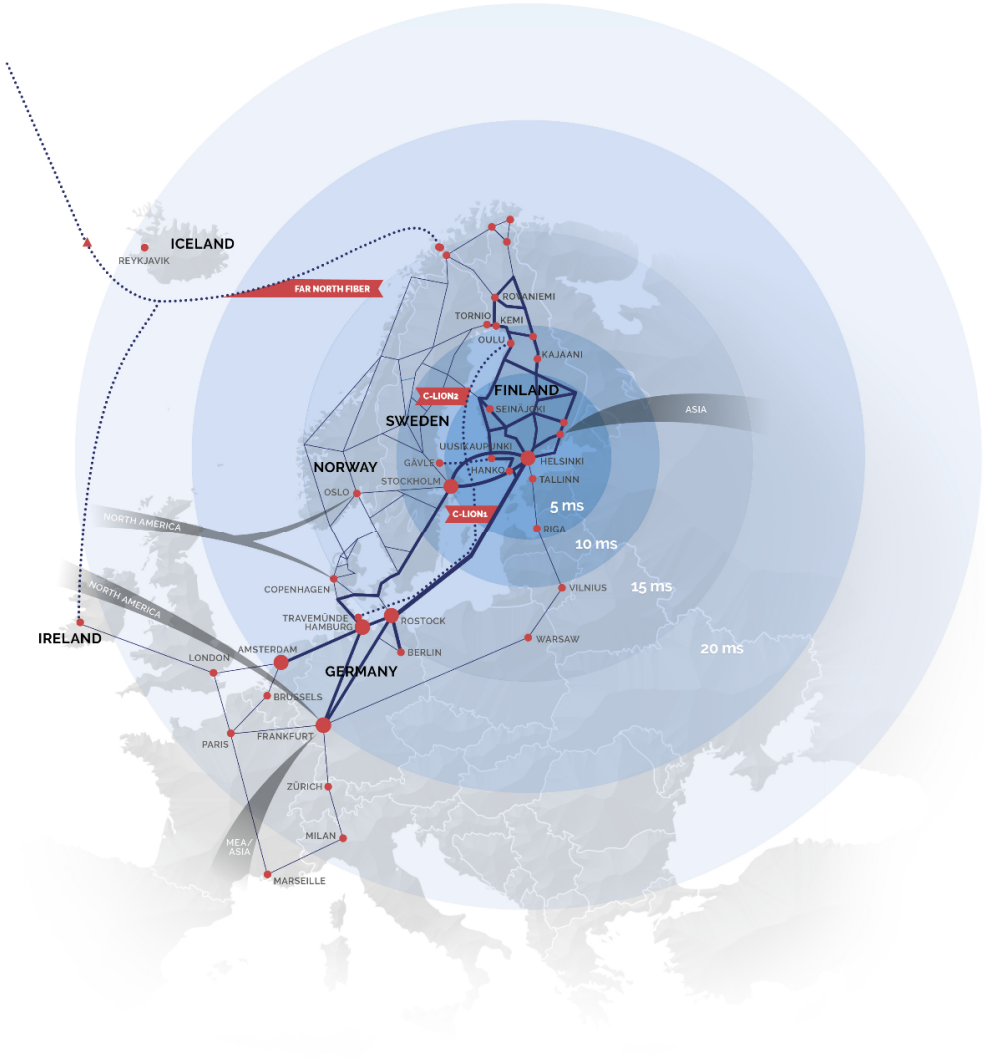
According to data provided by the Finnish National Bureau of Investigation, the damage to the pipeline was probably caused by the Chinese shipping company's Newnew Polar Bear, which continued its journey to Russian waters escorted by a Eurasian state icebreaker (Police of Finland, 2023a). In addition, the Sevmorput, a Russian nuclear-powered cargo ship, was also detected in the area during the incident (Police of Finland, 2023b).

Russia's alleged involvement in this attack could be aimed at destabilising the energy supply of these countries, which were heavily dependent on Russian gas until it was banned as a response to the invasion of Ukraine (Lietuvos Respublikos Energetikos Ministerija, 2022) (Latvijas Vēstnesis, 2022) (Republic of Estonia Ministry of Foreign Affairs, 2022) (Ministry of Economic Affairs and Employment of Finland, 2024). Already in 2014, in the Baltic States' attempts to expedite their disconnection from Russian supply through the synchronisation of their electricity grids with the support of the European Union (EU), Lithuania reported cases of interference by Russian military vessels in the installation of NordBalt, an undersea power cable connecting the country to Sweden (McNamara, 2024).

In November 2024, the submarine cable C-Lion1 , owned by the Finnish company Cinia, was apparently deliberately damaged. As this cable is essential for direct communication between Finland and Germany (see Figure 6), the damage resulted in the disruption of telecommunications between the two states. Such was the seriousness of the matter that the foreign ministers of these countries stated in a joint declaration that suspicions of an intentional attack were high, noting that "European security is not only threatened by Russia's war of aggression against Ukraine, but also by the hybrid warfare of malicious actors" and urging the strengthening of the defence of this type of infrastructure in the region (Ministry for Foreign Affairs of Finland, 2024).

Figure 6

Map of connectivity between the Nordic States and Central Europe via the C-Lion1 and C-Lion2 submarine cables.



Source: Cinia (n.d.)

Simultaneously, the BCS East-West Interlink telecommunications cable connecting Lithuania and Sweden was damaged as a result of "more than just an accident", as Andrius Šemeškevičius, Chief Technology Officer of the Telia Lietuva company, told Lithuanian national broadcaster LRT TV (2024).

The investigations undertaken by the countries concerned by both incidents focused on the Chinese vessel Yi Peng 3, which had previously departed from the Russian port of Ust-Luga. Unable to board the vessel, Danish naval forces kept a close eye on its situation once it entered the Kattegat Strait, as confirmed on their social media (Forsvaret, 2024). Based on Šemeškevičius' statements to LRT TV (2024), the likelihood of sabotage is quite high as the cables from both incidents intersect (see Figure 7).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

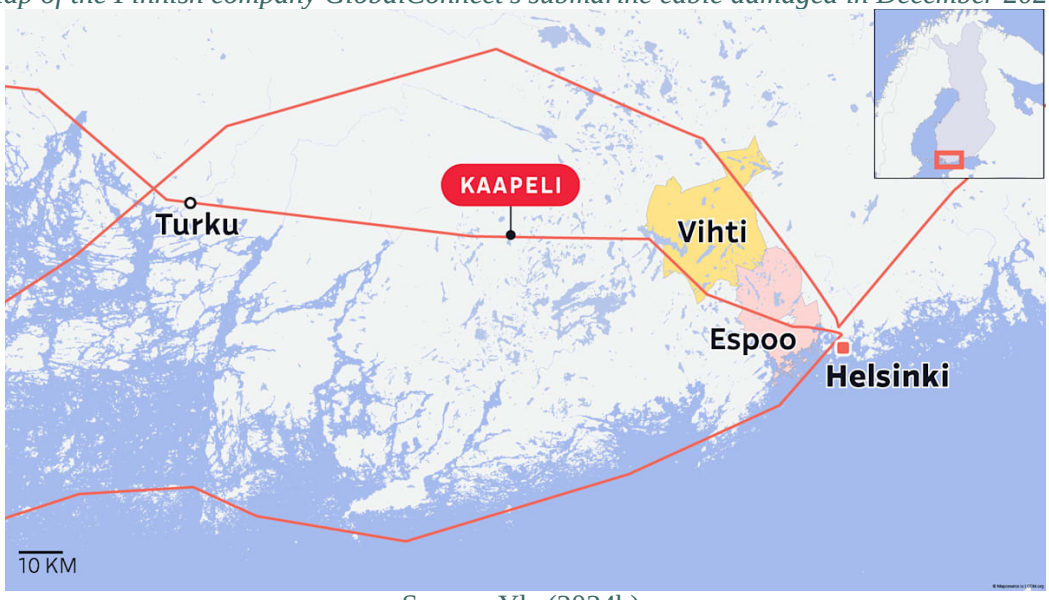
Figure 7
Map of damaged submarine cables in the Baltic Sea in November 2024 and the location of the vessel Yi Peng 3.

Source: Reuters (2024).

A month later, on 3 December 2024, the Finnish company GlobalConnect reported that its telecommunications cables connecting the country to Sweden had been damaged at two separate points between the Vithi and Espoo areas (see Figure 8), as confirmed by the company's communications manager, Niklas Ekström, to the Finnish public broadcaster Yle (2024a). However, the Finnish police said in a statement that there were no indications of sabotage, but rather an accident due to damage caused during excavations (Police of Finland, 2025a).

Figure 8

Map of the Finnish company GlobalConnect's submarine cable damaged in December 2024.

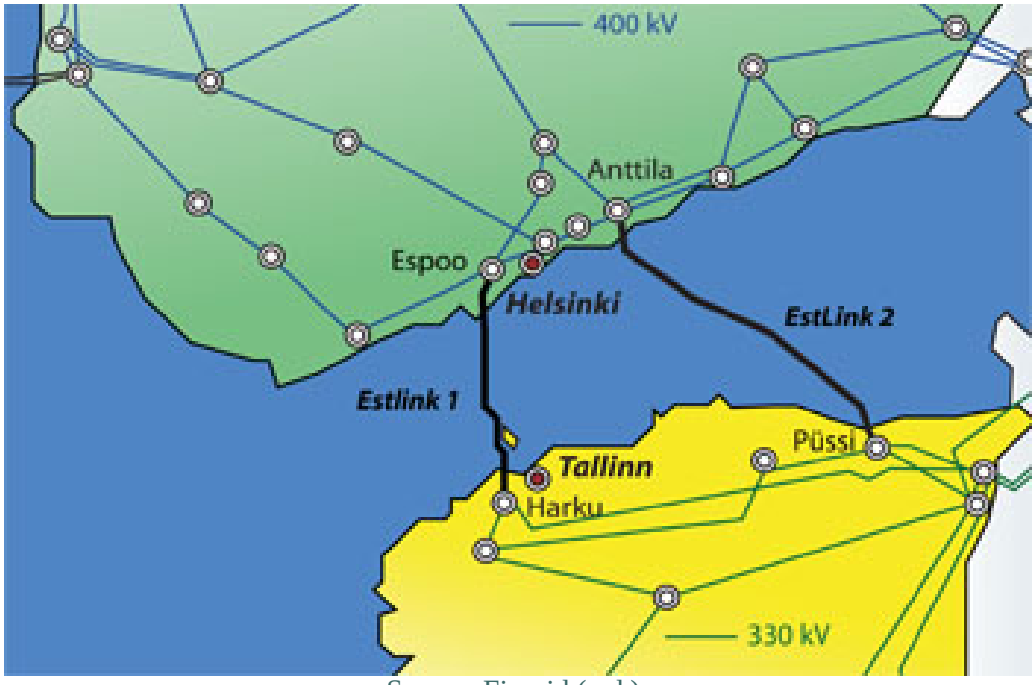


Source: Yle (2024b).

On 25 December 2024, the Finnish operator Fingrid reported that the Estlink 2 submarine cable of the electricity grid connecting Finland and Estonia was damaged (see Figure 9). Finland launched a sabotage investigation and seized the Russian "Ghost Fleet" tanker Eagle S, as it was in the area transporting Russian oil and apparently caused the damage by dragging its anchor (Police of Finland, 2025b). This event prompted NATO to announce in late December its intention to reinforce its military presence in the Baltic Sea to prevent future incidents and address possible new threats to this infrastructure (NATO, 2024a).

Figure 9

Map of connectivity between Finland and Estonia via the Estlink 1 and Estlink 2 submarine cables.



Source: Fingrid (n.d.).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

On 26 January 2025, damage was discovered to a communications cable between Sweden and Latvia (see Figure 10) as reported by the company responsible, Latvia State Radio and Television Center (2025). Although the Nordic country launched a preliminary investigation for sabotage and seized the Bulgarian cargo ship Vezhen, the Swedish prosecutor's office eventually determined that the cable break between the two countries was not the result of a deliberate attack but an accident (Swedish Prosecution Authority, 2025). Similarly, at the request of the Latvian authorities, Norway seized the Russian-crewed Silver Dania, which was sailing between St. Petersburg and Murmansk (Politiet, 2025).

Figure 10

Map of the submarine cable in the Baltic Sea connecting Latvia and Sweden damaged in January 2025.

Source: Reuters (2025).

In February 2025 another submarine cable connecting Finland and Germany was damaged in the Swedish EEZ, specifically near the Swedish island of Gotland. While Finland has already launched an investigation into the damage to the cable belonging to one of its companies (Police of Finland, 2025c), there is talk from Sweden of possible sabotage. Patrik Johansson, head of the Water and Sanitation Department in the affected region of Gotland, confirmed after the first inspection of the site that the main cause was human influence (Region Gotland, 2025).

Simultaneously, the Finnish company Cinia (2025) again reported disturbances in the operation of the C-Lion1 submarine cable. Although the investigation is still ongoing, the German media Kieler Nachrichten (2025) reported that the German authorities investigated the freighter Arne, a ship suspected of being part of the "Russian Ghost

Fleet", which was sailing in the area under the flag of Antigua and Barbuda and was heading from St. Petersburg to Seville without one of its anchors, raising suspicions of apparent Kremlin-orchestrated sabotage.

These incidents demonstrate that critical undersea infrastructure in the area is vulnerable to attack. Already in 2017, NATO Submarine Force Commander Andrew Lennon confirmed the existence of "Russian submarine activity in the vicinity of undersea cables" at previously unknown levels, highlighting Russia's strategic interest in NATO's undersea infrastructure (Birnbaum, 2017). As Monaghan et al. (2023, p. 1) note, these potential attacks are 'aimed at disrupting transatlantic cohesion and economic activity, undermining Western support for Ukraine, and shaping possible future military operations'. The situation since the outbreak of the war has therefore made security in this area a priority for NATO.

3. NATO AND THE PROTECTION OF CRITICAL UNDERSEA INFRASTRUCTURES

At a general level, the protection of critical undersea infrastructure for NATO is framed in several articles of its founding treaty. Specifically, article 2 on economic collaboration, article 3 on resilience and article 5 on collective defence from the North Atlantic Treaty (1949). With regard to the latter, NATO's New Strategic Concept (2022) mentions hybrid threats to critical infrastructure, reaffirming their inclusion in the framework of the aforementioned article and highlighting the commitment to international cooperation for their protection.

The growing concern for the protection of these infrastructures has made their security a particularly important objective for NATO. Given their importance for the functioning of society, threats such as the control acquired by Chinese companies over some of these infrastructures and the growing Russian activity near them made the Atlantic Alliance consider the state of its critical infrastructure in 2020 (García Pérez, 2023, p. 3).

Regarding the latter, then NATO Secretary General Jens Stoltenberg (2020) highlighted the importance of critical undersea infrastructure in the Alliance's efforts to strengthen its resilience:

> I think it's important to address this, because it is important to understand that most of these cables are privately owned and it's publicly known where they are. And that makes them potentially vulnerable. So we need to monitor the potential vulnerabilities. That's partly the reason why we have produced this report. We have tools to protect them and to monitor threats. And we have also established a new Atlantic Command in Norfolk, a new NATO command in Norfolk. And one of the tasks of this new North Atlantic Command is also to look into how to protect, how to monitor threats against undersea infrastructure. For instance, the internet is dependent on these cables and that just highlights the importance of the undersea cables. One of the main issues at the meeting today was resilience, and that's about civilian infrastructure, health services, telecommunications. But, of course, as part of our effort to strengthen the resilience, undersea cables, undersea infrastructure is an important part of that.

However, the main measures to protect these infrastructures were adopted after the start of the full-scale war in Ukraine in 2022. Until then, this issue was part of the work of limited institutions mostly linked to the maritime domain or to countering hybrid threats, two of which are particularly noteworthy.

On the one hand, the *Strengthened Resilience Commitment*, created in 2021 by a decision of NATO Heads of State and Government, which recognises the Alliance's commitment to intensify efforts to ensure the resilience of its critical infrastructures (NATO, 2021). On the other hand, the *NATO Resilience Committee,* a body responsible for the political-strategic direction, guidance, planning and overall coordination of resilience activities in the Atlantic Alliance (NATO, 2022) (see Table 1).

Table 1

NATO institutions in which critical infrastructure protection was framed ahead of Ukraine's full-scale war in 2022.

	Leading institutions
2006	*NATO Shipping Centre (NSC)*
2007	*Civil-Military Cooperation Centre of Excellence (CCOE)*
2008	*Cooperative Cyber Defence Centre of Excellence (CCD COE)*
2012	*NATO Allied Maritime Command (MARCOM)*
	Multinational Maritime Security Centre of Excellence (MARSEC COE)
2014	*Strategic Communications Centre of Excellence*
2018	*Counter Hybrid Support Teams*
2021	*Strengthened Resilience Commitment*
2022	*NATO Resilience Committee*

Source: Own elaboration based on information provided by NATO on its websites.

In response to the apparent sabotage of Nord Stream in late 2022, NATO established the *Critical Undersea Infrastructure Coordination Cell* (NATO, 2023a) in February 2023. A month before the adoption of this measure, on 11 January 2023, the creation of a NATO-EU working group on critical infrastructure resilience was announced in the framework of the existing NATO-EU Structured Dialogue on Resilience, within which it is embedded (European Commission & NATO, 2023, p. 2).

In their report published in June 2023, both sides point to the existence of a variety of threats to be faced, ranging from possible terrorist attacks to natural disasters. However, they directly point out that since the Russian aggression in Ukraine, these infrastructures have become a vulnerable asset whose protection must be a priority (European Commission & NATO, 2023, p. 4).

Another example of the effects of the Nord Stream incident as a turning point for strengthening Western efforts on the resilience of its critical undersea infrastructure is the creation of the *NATO Maritime Centre for the Security of Critical Undersea Infrastructure* (NMCSCUI) at the Vilnius Summit in 2023:

> The threat to critical undersea infrastructure is real and it is developing. We are committed to identifying and mitigating strategic vulnerabilities and

> dependencies with respect to our critical infrastructure, and to prepare for, deter and defend against the coercive use of energy and other hybrid tactics by state and non-state actors. Any deliberate attack against Allies' critical infrastructure will be met with a united and determined response; this applies also to critical undersea infrastructure. The protection of critical undersea infrastructure on Allies' territory remains a national responsibility, as well as a collective commitment. NATO stands ready to support Allies if and when requested. We have agreed to establish NATO's Maritime Centre for the Security of Critical Undersea Infrastructure within NATO's Maritime Command (MARCOM). We also agreed to set up a network that brings together NATO, Allies, private sector, and other relevant actors to improve information sharing and exchange best practice (NATO, 2023b).

In line with Stoltenberg (2020) and the joint report of the European Commission and NATO (2023, p. 3), the Vilnius Summit Communiqué reaffirms the Alliance's growing concern about threats to critical undersea infrastructure. In this extract, NATO recognises the need to proactively identify vulnerabilities, underlines that such threats can emanate from both state and non-state actors and stresses the importance of effective coordination with relevant actors, especially from the private sector. It also explicitly contemplates the possibility that hybrid attacks against these infrastructures could be considered as acts justifying the activation of Article 5 of the North Atlantic Treaty's collective defence.

The NMCSCUI was therefore inaugurated in May 2024. NATO defines it as a network and knowledge centre specialising in critical undersea infrastructure, whose main function is to support strategic decision-making processes, facilitate the operational deployment of forces and coordinate joint actions to ensure their protection. This is done through the integration of efforts between member states, strategic partners and the private sector (NATO Media Centre, 2024).

However, this is not the only measure resulting from the Vilnius Summit implemented by NATO to ensure that threats in the maritime domain are better addressed. In October 2023, the *Digital Ocean Vision*, an initiative aimed at improving maritime domain understanding by further harmonising national and allied maritime surveillance capabilities using a diverse range of assets, was adopted (NATO, 2023c).

Moreover, in view of the growing challenges to these infrastructures, on 23 May 2024 NATO held the first meeting of the Critical Undersea Infrastructure Network by decision of the defence ministers with the aim of improving coordination and information exchange. The meeting discussed measures such as strengthening naval patrols, promoting technological innovation and the use of advanced detection and response capabilities, consolidating the Alliance's central role in this area (NATO, 2024b).

In November 2024, Exercise *Bold Machina 24* was conducted in La Spezia, Italy, coordinated by the *Allied Special Operations Forces Command* (SOFCOM) and the *Centre for Maritime Research and Experimentation* (CMRE) with the aim of testing underwater sensors for critical infrastructure protection (NATO Centre for Maritime Research and Experimentation, 2024, p. 2). Such exercises reflect the aforementioned interest in integrating emerging technologies, such as unmanned systems, to enhance security in the undersea domain (Conte de los Ríos, 2025, p. 26).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

In this regard, it is also noteworthy that NATO has developed new tools that enable allies to detect suspicious activity in order to protect against sabotage. These include the use of artificial intelligence as exemplified by *Mainsail*, a software tool developed by CEMR that detects vessels behaving suspiciously with the intention of gathering information about and damaging undersea infrastructure (NATO Multimedia, 2025).

With regard to the specific protection of the Baltic Sea's undersea infrastructure, NATO has promoted the technological innovation necessary for effective detection of any suspicious activity to complement the work of its patrols in the region. These measures have been progressively intensified as a direct consequence of the apparent sabotage of Nord Stream, as the Alliance itself acknowledges (NATO, 2023d).

In February 2025, NATO conducted a demonstration of unmanned surface vehicles (USVs) in the Baltic Sea in order to advance their operational integration in maritime surveillance tasks. This initiative is part of the Alliance's efforts to incorporate emerging and disruptive technologies - such as autonomous systems and artificial intelligence - aimed at optimising situational awareness and strengthening the protection of critical undersea infrastructure, in particular along sea lines of communication (NATO Allied Maritime Command, 2025b). Furthermore, in the framework of the Resilience Committee, NATO presented its first *Resilience Reference Curriculum* in 2025 with the aim of strengthening allied capabilities against threats, including those targeting critical infrastructure (NATO, 2025a).

At the same time, cooperation with the European Union has gained importance through initiatives such as the *EU Hybrid Toolbox*, the *Hybrid Fusion Cell* and the *Hybrid Rapid Response Teams*, designed to promote synergies and strengthen anti-hybrid coordination with NATO (European External Action Service, 2022, p. 34). This convergence of initiatives between the above-mentioned entities demonstrates the importance of developing robust defensive capabilities, and their coordinated implementation together with the effective integration of new technologies and operational capabilities is essential to ensure the successful protection of European submarine infrastructures, especially in view of the rapidly evolving threats affecting this area (Conte de los Ríos, 2025, p. 33).

Finally, it should be noted that NATO considers strengthening cooperation with the private sector as a key dimension of improving its ability to respond to threats to critical undersea infrastructures. This cooperation is justified, on the one hand, by the fact that a significant proportion of such infrastructure is privately owned or operated, and on the other hand, by the potential of the private sector to provide essential technological solutions in an increasingly complex operating environment (Fridbertsson, 2023, p. 11).

4. OPERATION BALTIC SENTRY

On 14 January 2025, NATO held a Baltic Sea Allies Summit to address the growing threats to the region's critical undersea infrastructure. As a result, the Atlantic Alliance Secretary General and participants issued the *Joint Statement of the Baltic Sea NATO Allies Summit* (2025) announcing the launch of a military initiative aimed at strengthening the protection of this infrastructure: Operation *Baltic Sentry.*

Citing deep concern over the increase in actions that threaten the operation of critical undersea infrastructure, the Alliance signalled its readiness to "deter, detect and counter any attempted sabotage" and to respond to any attack "with a firm and decisive response" (Tasavallan Presidentti, 2025). This comes at a time when NATO recognises the need to modernise its capabilities to strengthen its deterrence and defence in order to address and counter evolving security threats (Tasavallan Presidentti, 2025).

MARCOM, under the direction of the *Joint Forces Command* Brunssum (JFCBS), is recognised as playing a key role in coordinating operations within what it defines as a "multi-domain surveillance activity aimed at increasing maritime situational awareness in the Baltic Sea to deter and defend against attacks on critical undersea infrastructure" (NATO Allied Maritime Command, 2025a). To that end, Operation *Baltic Sentry* includes the deployment of additional sea, air and land assets by allies to enhance surveillance and deterrence.

By conducting regular patrols and joint exercises, NATO seeks to maintain a constant presence in the Baltic Sea that is continuously monitored by warships, submarines, aircraft and the support of advanced maritime surveillance technology. For example, ships from *Standing NATO Maritime Group 1* (SNMG1) and *Standing NATO Mine Countermeasures Group 1* (SNMCMG1) will participate in *Baltic Sentry* alongside other allied maritime patrol vessels, while NATO will continue to invest in cutting-edge military technology to detect and minimise threats such as artificial intelligence, advanced sensors and specialised sonar systems (MARCOM, 2025).

This is in addition to the inclusion of two key actors within the Alliance. On the one hand, the recently inaugurated *Commander Task Force* (CTF) in the Baltic Sea itself, based in the port city of Rostock. In addition to coordinating allied ships in the Baltic, the CTF works to build a unified regional vision for critical infrastructure in the Baltic Sea in order to support NATO's strategic protection efforts (Tasavallan Presidentti, 2025). On the other, the aforementioned NMCSCUI will focus its efforts on protecting and securing vital submarine assets (Tasavallan Presidentti, 2025).

To achieve these goals, NATO considers it essential not only to work within the Alliance itself, but also to collaborate and cooperate with other actors ranging from the EU to the private sector. While in the former case cooperation will focus on strengthening existing mechanisms, in the case of the private sector NATO stresses the importance of cooperating with infrastructure operators and cutting-edge technology companies in developing the different response measures needed to increase resilience (Tasavallan Presidentti, 2025).

The Atlantic Alliance also envisages the adoption of new measures in accordance with international law, aimed at both prevention and response to threats or irresponsible acts against critical undersea infrastructures in the region (Tasavallan Presidentti, 2025). In the framework of the launch of Operation *Baltic Sentry*, the current NATO Secretary General Mark Rutte underlined the need for strict enforcement of the existing legal framework, warning that any potential threat against these infrastructures could lead to coercive measures such as boarding, seizure or detention of vessels. In this context, he pointed to Finland's response to incidents as an outstanding example of action (NATO, 2025b).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

The implementation of these measures is justified by the constant mention of the existence of threats. With regard to the latter, one threat in particular is mentioned, the so-called "Russian Ghost Fleet". This is defined as a significant threat to maritime and environmental security both in the Baltic Sea region and globally, as it compromises the integrity of underwater infrastructure, increases the risks associated with chemical munitions dumped on the seabed and represents a major source of funding for Russia's illegal war of aggression against Ukraine (Tasavallan Presidentti, 2025).

Similarly, it is recognised that the threat to critical undersea infrastructures is not limited to the Baltic Sea. It therefore points out that Operation *Baltic Sentry* also represents a turning point in favour of greater cooperation to strengthen the resilience of these critical infrastructures and, therefore, to strengthen NATO's security. Hence, the launch of the operation itself goes hand in hand with the announcement of the renewal of the alliance's maritime strategy (Tasavallan Presidentti, 2025).

5. CONCLUSIONS AND PROPOSALS

Critical undersea infrastructures are vital for the economy and the global communications system. Their growing importance and the constant technological advances in this area have made them a priority target for defence, but also for possible attacks. In this way, *Seabed Warfare* is no longer a distant concept, but an immediate threat to the Allies. The close link between the security of these infrastructures and global stability, particularly in economic and communications terms, means that protecting them and managing their vulnerabilities is now a defence priority for all international actors.

Given the current context of rivalry with a Russia that publicly announces its desire to destabilise NATO, this makes the implementation of critical infrastructure protection strategies an extremely urgent objective for the defence of the Atlantic Alliance, especially in the Baltic region. As mentioned in the paper, the Baltic Sea is not only an enclave of geopolitical competition between NATO and Russia, but also a key area for the security of critical undersea infrastructures that guarantee the stability of the Allies. Joining forces in this region to strengthen its security must therefore be a priority for NATO, especially since the 2022 war in Ukraine and the accession of Sweden and Finland to the Alliance.

This allows us to draw the main conclusion linked to specific objective number one of this study. While the protection of these infrastructures should already be an objective for NATO given their importance for the resilience of society and their extreme vulnerability to a wide range of threats, the current geopolitical situation makes these infrastructures a clear target for possible attacks. This is demonstrated by the increase in incidents involving submarine cables in the Baltic Sea since the start of the conflict in 2022, with eight incidents to date in which critical infrastructures in the region have been damaged, practically all of them occurring within the EEZ of Finland and Sweden, countries that coincidentally applied to join NATO that same year despite fierce opposition from the Kremlin (see Table 2).

Table 2

Incidents in the critical underwater infrastructure in the Baltic Sea since 2022.

	Infrastructure	**Location of the incident**	**Countries affected**	**Causes**
Nord Stream	Subsea pipeline	Swedish and Danish EEZs	European Union	High indications of sabotage
Balticconnector	Subsea pipeline	Finnish EEZ	Finland and Estonia	High indications of sabotage
C-Lion 1	Telecommunications cable	Swedish EEZ	Finland and Germany	High indications of sabotage
BCS East-West Interlink	Telecommunications Cable	Swedish EEZ	Lithuania and Sweden	High indications of sabotage
GlobalConnect	Telecommunication cables	Finnish EEZ	Finland and Sweden	Accident
Estlink 2	Electricity grid	Swedish EEZ	Finland and Estonia	High indications of sabotage
Latvia State Radio and Television Center	Telecommunications cable	Swedish EEZ	Sweden and Latvia	Accident
Gotland	Maritime cable owned by a Finnish company	Swedish EEZ	Finland and Germany	High indications of sabotage

Source: Own elaboration

With regard to the second specific objective of this study on NATO's overall framework for action in protecting critical undersea infrastructure, several conclusions can be drawn. Despite the Russian military's attrition in its performance in the Ukrainian war and the severe setbacks suffered in the naval domain, Russian hybrid tactics remain the most pressing threat to European infrastructure in the Baltic Sea. NATO is positioning itself as a central actor in preventing attacks against such infrastructure, stepping up its efforts with progressive measures from 2022 onwards following the invasion of Ukraine and subsequent incidents.

While this issue was part of the work of mostly maritime-related institutions, since the apparent sabotage of Nord Stream - in the midst of tensions with Moscow - NATO has adopted almost a dozen measures. These include the creation of the *Critical Undersea Infrastructure Coordination Cell* or the *NATO Maritime Centre for the Security of Critical Undersea Infrastructure*, the *Digital Ocean Vision* initiative, military exercises such as *Bold Machina 24*, the technological innovation necessary to take advantage of artificial intelligence such as *Mainsail*, and the adoption of complementary initiatives with third actors such as the EU.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Operation *Baltic Sentry* is NATO's main response to the challenge of protecting critical undersea infrastructure in the Baltic Sea and strengthening security in the region. In keeping with the main objective of the study focused on analysing this operation, it can be observed that the measures implemented within its framework are geared towards strengthening detection, deterrence-prevention, adaptation and response capabilities, thus being in line with the main criteria proposed by the specialised literature for adopting an effective strategy (see Table 3).

Table 3

Implementation of the necessary elements for an effective strategy for the protection of critical undersea infrastructure in the framework of NATO's Operation Baltic Sentry.

	NATO Operation Baltic Sentry
Increased presence or surveillance	✓
Collaboration with international actors	✓
Coordination with the private sector	✓
Use of advanced technology	✓
Development of regulatory frameworks	✓
Renewal of the maritime strategy	✓
Implementation of response measures	✓

Source: Own elaboration based on Conte de los Ríos (2025), Monaghan et al. (2023), Fridbertsson (2023) and information provided by NATO.

In short, Operation *Baltic Sentry* demonstrates that critical undersea infrastructures are currently identified by NATO as a strategic vulnerability whose protection is essential to ensure the resilience and security not only of the Alliance, but also for the day-to-day life of society. A lesson that finds a turning point in the different episodes that have occurred in the framework of the war in Ukraine since 2022, with the apparent attack on Nord Stream at the end of the same year being noteworthy, as shown both by the chronological framework of the measures adopted by NATO in this sector and by the Alliance itself when justifying the latter.

Thus, answering the overall research question, the general hypothesis of the study is that Operation *Baltic Sentry* enhances the protection of critical undersea infrastructure in the Baltic Sea and the Alliance's presence in the Baltic Sea, thus adjusting to the new threat context.

BIBLIOGRAPHICAL REFERENCES

Arjona Hernández, N. (2023). The protection of submarine telecommunications cables: Digital sovereignties and submarine cable network security. *International Journal Of Policy Thinking*, *18*(18), pp. 41-67. https://doi.org/10.46661/revintpensampolit.8753

Baltic Marine Environment Protection Commission (2024). *HELCOM Map and Data Service*. https://maps.helcom.fi/website/mapservice/

Baltic Marine Environment Protection Commission (2024). *HELCOM Map and Data Service*. https://maps.helcom.fi/website/mapservice/

Birnbaum, M. (22 December 2017). Russian submarines are prowling around vital undersea cables. It's making NATO nervous. *The Washington Post.* https://www.*washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?hpid=hp_hp-top-table-main_russiasubs712pm%3Ahomepage%2Fstory*

Bueger, C., Liebetrau, T., and Franken, J. (2022). *Security Threats to Undersea Communications Cables and Infrastructure - Consequences for the EU*. European Parliament In-Depth Analysis, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Bueger, C., and Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, *42*(3), pp. 391-413. https://doi.org/10.1080/13523260.2021.1907129

Cassetta, M. (2024). How to Respond to the Emerging Threats to Critical Underwater Infrastructure at the Time of Russia's War Against Ukraine. *Istituto Affari Internazionali (IAI), IAI Commentaries 24-31 June 2024*, pp. 1-5. https://www.iai.it/en/pubblicazioni/c05/how-respond-emerging-threats-critical-underwater-infrastructure

Childs, N. (2025). Russia's 'Shadow Fleet' and Sanctions Evasion: What Is To Be Done? *The International Institute for Strategic Studies (IISS), January 2025*, pp. 1-15. https://www.iiss.org/globalassets/media-library---content--

migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf

Cinia (20 February 2025). *Disturbance in Cinia's C-Lion Submarine Cable.* https://www.cinia.fi/en/news/disturbance-in-cinia-c-lion-submarine-cable

Cinia (n.d.). *International connectivity by Cinia.* https://www.cinia.fi/hubfs/Cinia%20Theme%202024/Muut%20kuvat/Cinian-kansainvaliset-verkkoyhteydet-kartta.jpg

Clark, B. (2015). *The Emerging Era in Undersea Warfare*. Center for Strategic and Bidgetary Assessments (CSBA), https://csbaonline.org/research/publications/undersea-warfare

Conte de los Ríos, A. (2025). Security threats: seabed and critical infrastructure. *Global Affairs Journal*, (7), pp. 26-35. https://www.unav.edu/documents/16800098/147587031/amenazas-seguridad.pdf

Deni, J. R. (18 December 2023). *Is the Baltic Sea a NATO Lake?* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/is-the-baltic-sea-a-nato-lake?lang=en

Energistyrelsen (26 September 2022). *Leak at North Stream 2 in the Baltic Sea.* https://ens.dk/en/press/leak-north-stream-2-baltic-sea

European Commission & NATO . (2023). *EU-NATO TASK OF FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE. FINAL ASSESMENT REPORT.* https://www.nato.int/cps/en/natohq/news_216631.htm

European External Action Service (2022). *A STRATEGIC COMPASS FOR SECURITY AND DEFENCE: For a European Union that protects its citizens, values and interests and contributes to international peace and security.* https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Fingrid (n.d.). *EstLink 2 - second high-voltage direct current link between Finland and Estonia.* https://www.fingrid.fi/en/grid/construction/arkisto/estlink-2/

Fink, A. and Kofman, M. (2020). Russian Strategy for Escalation Management: Key Debates and Players in Military Thought. *CNA Information Memorandum, April 2020*, pp. 1-48. https://www.cna.org/cna_files/pdf/DIM-2020-U-026101-Final.pdf

Foggo, J. (17 January 2023). The Fourth Battle of the Atlantic Is Underway. *Center for European Policy Analysis (CEPA)*, https://cepa.org/article/the-fourth-battle-of-the-atlantic-is-underway/

Foggo, J. and Fritz, A. (2016). The Fourth Battle of the Atlantic. *U.S. Naval Institute, 142*(6), https://www.usni.org/magazines/proceedings/2016/june/fourth-battle-atlantic

Forsvaret. [@forsvaretdk] (20 November 2024). *Regarding the Chinese ship Yi Peng 3: The Danish Defence can confirm that we are present in the area near the Chinese ship Yi Peng 3. The Danish Defence currently has no further comments.* [Post in X]. X. https://x.com/forsvaretdk/status/1859195509866381402

Fridbertsson, N. T. (2023). *Protecting Critical Maritime Infrastructure - The Role of Technology*. General Report. 032 STC 23 E. NATO Parliamentary Assembly: Science and Technology Committee (STC). https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc

García Pérez, R. (2023). Spain in the global network of submarine cables. *Instituto Español de Estudios Estratégicos, IEEE Framework Document 10/2023*, pp. 1-51. https://www.defensa.gob.es/ceseden/-/espa%C3%B1a-en-la-red-global-de-cables-submarinos

García Pérez, R. (2024). "La seguridad de los cables submarinos", in Fernándo Ibáñez Gómez (Coord.), *Seguridad marítima. Una incertidumbre permanente*, Bosch Editor, Barcelona, pp. 265-298.

Gasgrid (n.d.). *Map of Finnish and Baltic gas transmissions.* https://gasgrid.fi/wp-content/uploads/Gasgrid_maakaasu_lisaversiot_eu_EN-scaled.jpg

Gasum (2023). *Gasum has terminated its pipeline natural gas supply contract with Gazprom Export. https://www.gasum.com/en/news-and-customer-stories/news-and-press-releases/2023/gasum-has-terminated-its-pipeline-natural-gas-supply-contract-with-gazprom-*

export/#:~:text=The%20parties%20were%20not%20able,details%20of%20the%20contract%20termination.

Gresh, G. F. (2023). *Europe's new maritime security reality: Chinese ports, Russian bases, and the rise of subsea warfare.* Foreign Policy at Brookings, Policy Brief, February 2023. https://www.brookings.edu/articles/europes-new-maritime-security-reality-chinese-ports-russian-bases-and-the-rise-of-subsea-warfare/

Guilfoyle, D., Paige, T. P., and McLaughlin, R. (2022). THE FINAL FRONTIER OF CYBERSPACE: THE SEABED BEYOND NATIONAL JURISDICTION AND THE PROTECTION OF SUBMARINE CABLES. *International and Comparative Law Quarterly*, *71*(3), pp. 657-696. https://doi.org/10.1017/S0020589322000227

Insikt Group (2023). *The Escalating Global Risk Environment for Submarine Cables.* Recorded Future Threat Analysis, https://www.recordedfuture.com/research/escalating-global-risk-environment-submarine-cables

International Cable Protection Committee (2024). *Report of the International Cable Protection Committee Docs: HSSC16-07.10A: ICPC activities affecting HSSC.* International Hydrographic Organization, Tokyo, Japan, 27-31 May 2024. https://iho.int/uploads/user/Services%20and%20Standards/HSSC/HSSC16/HSSC16_2024_07.10A_EN_ICPC%20activities%20affecting%20HSSC.pdf

Jones, S. G. (2025). Russia's Shadow War Against the West. *Center for Strategic and International Studies (CSIS), CSIS Briefs March 2025*, pp. 1-20. https://www.csis.org/analysis/russias-shadow-war-against-west

Kaushal, S. (25 May 2023). *Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure*. Royal United Services Institute (RUSI), May 2023. https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure

Kieler Nachrichten (2025). *Verdacht der Sabotage: Ermittler suchen Anker vom russischen Frachter "Arne"* [Suspicion of *sabotage*: Investigators *search for* the anchor of the Russian freighter "Arne"]. https://www.kn-online.de/schleswig-holstein/verdacht-der-sabotage-gegen-russischen-frachter-arne-in-kiel-ermittlungsstand-ORSQRUDZZRGJHC7KSCB4SKJCDM.html

Latvia State Radio and Television Center (2025). *LVRTC Submarine Optical Fiber Cable Damaged.* https://www.lvrtc.lv/en/news/jaunumi/lvrtc-submarine-optical-fiber-cable-damaged/

Latvijas Vēstnesis (28 July 2022). *Grozījumi Enerģētikas likumā* [Energy Law Amendments]. https://www.vestnesis.lv/op/2022/144.5

Lietuvos Respublikos Energetikos Ministerija (20 May 2022). *No more Russian oil, gas and electricity imports in Lithuania from Sunday.* https://enmin.lrv.lt/en/news/no-more-russian-oil-gas-and-electricity-imports-in-lithuania-from-sunday/

LRT TV (18 November 2024). *Undersea cable between Lithuania and Sweden damaged - Telia.* https://www.*lrt.lt/en/news-in-english/19/2416006/undersea-cable-between-lithuania-and-sweden-damaged-telia?srsltid=AfmBOoowPquC_SbY0w-dUT2dfxJTzPrj-OPvif6IxXoDTJQuKnQx11fF*

McNamara, E. M. (17 March 2016). *Securing the Nordic-Baltic region*. NATO Review. https://www.nato.int/docu/review/articles/2016/03/17/securing-the-nordic-baltic-region/index.html

McNamara, E. M. (28 August 2024). Strengthening resilience: NATO's role in enhancing the security of critical undersea infrastructures. *NATO Review: Opinion, Analysis and debate on Security Issues*, https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html

Ministry for Foreign Affairs of Finland (18 November 2024*). Joint statement by the Foreign Ministers of Finland and Germany on the severed undersea cable in the Baltic Sea.* https://um.fi/statements/-/asset_publisher/6zHpMjnolHgl/content/joint-statement-by-the-foreign-ministers-of-finland-and-germany-on-the-severed-undersea-cable-in-the-baltic-sea/35732

Ministry of Economic Affairs and Employment of Finland (7 May 2024). *Hallituksen esitys laiksi laiksi maakaasun ja nesteytetyn maakaasun maahantuonnin väliaikaisesta kieltämisestä Venäjän federaatiosta ja Valko-Venäjältä* [The government's proposal for a law on the temporary ban on the import of natural gas and liquefied natural gas from the Russian Federation and Belarus]. https://tem.fi/en/project?tunnus=TEM036:00/2024

Monaghan, S. (6 October 2022). Five Steps NATO Should Take after the Nord Stream Pipeline Attack. *Center for Strategic and International Studies (CSIS),* https://www.csis.org/analysis/five-steps-nato-should-take-after-nord-stream-pipeline-attack

NATO Allied Maritime Command (2025a, 14 January 2025). *NATO's Baltic Sentry steps up patrols in the Baltic Sea to safeguard Critical Undersea Infrastructure*. https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure

NATO Allied Maritime Command (2025b, 20 February 2025). *NATO Conducts Unmanned Surface Vehicle Demonstration in Baltic Sea.* https://mc.nato.int/media-centre/news/2025/page228602539

NATO Centre for Maritime Research and Experimentation (2024). *NATO STO CMRE NEWSLETTER.* January-June 2024. https://www.cmre.nato.int/wp-content/uploads/2024/09/v2%20NATO%20STO%20CMRE%20Newsletter_1_20240712_114854_0000_EDITED_4PAGES%20(002).pdf

NATO Media Centre (2024, 28 May 2024). *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure.* https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

NATO Multimedia (06 February 2025). *Protecting undersea cables with artificial intelligence.* https://www.natomultimedia.tv/app/asset/718197

NATO (2021, 14 June 2021). *Strengthened Resilience Commitment.* https://www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO (2022, 07 October 2022). *Resilience Committee*. https://www.nato.int/cps/in/natohq/topics_50093.htm

NATO (2023a, 15 February 2023). *NATO stands up undersea infrastructure coordination* cell. https://www.nato.int/cps/en/natohq/news_211919.htm

NATO (2023b, 11 July 2023). *Vilnius Summit Communiqué. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023.* https://www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO (2023c, 12 October 2023). *NATO Defence Ministers launch initiative to enhance maritime surveillance capabilities.* https://www.nato.int/cps/ra/natohq/news_219441.htm

NATO (2023d, 19 October 2023). *NATO steps up Baltic Sea patrols after subsea infrastructure damage.* https://www.nato.int/cps/en/natohq/news_219500.htm

NATO (2024a, 30 December 2024). *NATO to enhance military presence in the Baltic Sea.* https://www.nato.int/cps/en/natohq/news_231800.htm

NATO (2024b, 23 May 2024). *NATO holds first meeting of Critical Undersea Infrastructure Network.* https://www.nato.int/cps/en/natohq/news_225582.htm

NATO (2025a, 21 February 2025). *NATO launches the Resilience Reference Curriculum.* https://www.nato.int/cps/en/natohq/news_233458.htm

NATO (2025b, 14 January 2025). *NATO launches 'Baltic Sentry' to increase critical infrastructure security.* https://www.nato.int/cps/en/natohq/news_232122.htm

Police of Finland (2025b, 2 March 2025). *Eagle S tanker to move to international waters under Border Guard's control.* https://poliisi.fi/en/-/eagle-s-tanker-to-move-to-international-waters-under-border-guard-s-control

Police of Finland (2023a, 24 October 2023). *National Bureau of Investigation has technically clarified the cause of gas pipeline damage.* https://poliisi.fi/en/-/national-bureau-of-investigation-has-clarified-technically-the-cause-of-gas-pipeline-damage

Police of Finland (2023b, 17 October 2023). *National Bureau of Investigation examines background of vessels sailing in the gas pipeline damage area.* https://poliisi.fi/en/-/national-bureau-of-investigation-examines-background-of-vessels-sailing-in-the-gas-pipeline-damage-area

Police of Finland. (2025a, 3 December 2025). *Police do not suspect any criminal offence in either of the cable damage incidents in Southern Finland.* https://poliisi.fi/en/-/police-do-not-suspect-any-criminal-offence-in-either-of-the-cable-damage-incidents-in-southern-finland

Police of Finland (2025c, 21 February 2025). *National Bureau of Investigation to conduct a preliminary inquiry into suspected cable damage in Baltic Sea.*

https://poliisi.fi/en/-/national-bureau-of-investigation-to-conduct-a-preliminary-inquiry-into-suspected-cable-damage-in-baltic-sea

Politiet (31 January 2025). *Ship can leave Tromsø.* https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2025/01/31/troms2/

Quijarro Santibáñez, L. (2023). Seabed Warfare: Submarine Warfare in the 21st Century. *Revista de Marina, 141*(997), pp. *15-22*. https://revistamarina.*cl/revista/997*

Region Gotland (3 March 2025). *Misstänkt sabotage* [Suspected sabotage]. https://gotland.se/bygga-bo-och-miljo/vatten-och-avlopp/dricksvatten/misstankt-sabotage

Republic of Estonia Ministry of Foreign Affairs . (2022). *Estonia imposes a ban on natural gas imports and purchases from Russia.* https://www.vm.ee/en/news/estonia-imposes-ban-natural-gas-imports-and-purchases-russia

Reuters (2024). *Damaged fibre-optic cables in the Baltic Sea.* https://www.reuters.com/graphics/BALTICSEA-CABLES/zdpxqaaxwvx/chart.png

Reuters (2025). *Damaged fibre-optic cable in the Baltic Sea*. https://www.reuters.com/graphics/BALTIC-SECURITY/xmvjbdamavr/chart.png

Stoltenberg, J. (22 October 2020). *Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers.* https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

Submarine Telecoms Forum (2025). *Global Outlook.* SubTel Forum Magazine #140. https://subtelforum.com/subtel-forum-magazine-140-global-outlook/

Swedish Prosecution Authority (2025). *Prosecutor revokes decision on seized ship.* https://www.aklagare.se/en/media/press-releases/2025/february/prosecutor-revokes-decision-on-seized-ship/?_t_id=ajCngOfkVK4qcLdxSmm4EA%3d%3d&_t_uuid=ajbjBKKES7uVHPgMJkVsvA&_t_q=baltic&_t_tags=language%3aen%2csiteid%3a764c28f6-3ce5-48e7-a8ec-b8f5f22e4245%2candquerymatch&_t_hit.id=Aklagare_Web_Business_PressRel

eases_Models_PressReleasePage/_847c0fdb-df1d-4d16-9b4a-0db494be3af4_en&_t_hit.pos=2

Tasavallan Presidentti (14 January 2025). *Joint Statement of the Baltic Sea NATO Allies Summit.* https://www.presidentti.fi/joint-statement-of-the-baltic-sea-nato-allies-summit/

The European Space Agency (06 October 2022). *Nordstream pipeline map with shipping traffic.* https://www.esa.int/ESA_Multimedia/Images/2022/10/Nordstream_pipeline_map_with_shipping_traffic

Yle (2024a, 31 December 2024). *Police: No crime suspected in Finland-Sweden cable break.* https://yle.fi/a/74-20128835

Yle. (2024b). *The cable was damaged in two separate places between Espoo and Vihti. Image: Laura Merikalla / Yle, Mapcreator, OpenStreetMap, GlobalConnect.* https://images.cdn.yle.fi/image/upload/c_crop,h_1080,w_1919,x_0,y_0/ar_1.7777777777777777,c_fill,g_faces,h_675,w_1200/dpr_2.0/q_auto:eco/f_auto/fl_lossy/v1733216443/39-1389673674ec7f18a492

REGULATION

United Nations Convention on the Law of the Sea, New York, 30 April 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf

Convention for the Protection of Submarine Telegraph Cables, Paris, 14 March 1884. https://iscpc.org/information/Convention_on_Protection%20_of_Cables_1884.pdf

NATO's New Strategic Concept, Madrid, 29 June 2022. https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

North Atlantic Treaty, Washington, 4 April 1949. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra