



BRIEFING  
PAPER

**404**

February 2025

# The EU and NATO in pursuit of better deterrence

Baltic Sea sabotage prompts rethink  
of current practices

Teemu Tammikko

**FIIA**

FINNISH  
INSTITUTE OF  
INTERNATIONAL  
AFFAIRS

**BRIEFING PAPER 404 / February 2025**

# **The EU and NATO in pursuit of better deterrence**

## Baltic Sea sabotage prompts rethink of current practices

### **Summary**

- Recurring incidents damaging critical undersea infrastructure in the Baltic Sea underline the need for better ways to deter destabilizing acts, whether intentional or due to negligence.
- These incidents should be viewed within the wider context of hybrid interference in the region, including the use of the so-called Russian shadow fleet. Responses should form a comprehensive and coherent set of actions targeting both state and non-state actors behind the interference.
- To improve accountability and attribution regarding damage, affected states should aim to agree on a common operational protocol for pursuing and investigating suspected vessels, and invest more in surveillance and detection capabilities, including emerging disruptive technologies.
- There is no silver bullet for improving deterrence within existing legal and political frameworks, but several smaller measures could help increase the costs of destabilizing acts. For instance, the EU could use its regulatory power as well as trade and economic tools to penalize those linked to the incidents, including, when appropriate, ship captains and crew, owners, flag states, and relevant port states.

### **Author**



**Teemu Tammikko**

Senior Research Fellow  
The European Union and Strategic  
Competition  
FIIA

## Introduction

There are thousands of kilometres of cables and pipelines on the seabed of all seas, including the Baltic Sea, which has recently experienced numerous disruptions to its undersea infrastructure. Their locations are often accessible through open sources, and responsibility for their surveillance and incident response is typically divided among several coastal states and private companies that own the infrastructure. This division leaves gaps, especially when it comes to information sharing and competences regarding the response. This is particularly true in international waters, where the United Nations Convention on the Law of the Sea (UNCLOS) allows passage for practically any type of vessel. As a result, the infrastructure is particularly vulnerable to both natural and human-induced incidents.

In recent years, both the EU and NATO have focused heavily on enhancing the resilience of undersea infrastructure.<sup>1</sup> Following the Nord Stream sabotage in 2022, streamlining operational processes<sup>2</sup> and finding synergies in EU-NATO cooperation<sup>3</sup> became even more important. This means that, in the event of disruptions, alternative networks should ensure security of supply, and that there are ways to mitigate the impact both nationally and across borders, as well as to swiftly repair any damage. Resilience has been viewed as *deterrence by denial*, meaning that if the level of harm is low, causing intentional damage would not be worthwhile.

- 1 E.g., Critical Entities Resilience (2022/2557) and Network and Information Security 2 (2022/2555) Directives; NATO “Seven Baseline Requirements” (Seven baseline requirements - CIMIC Handbook).
- 2 Council of the European Union: “Council Recommendation on a Blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance”, 10653/24.
- 3 EU-NATO Task Force on the Resilience of Critical Infrastructure: [EU-NATO Task Force on the resilience of critical infrastructure: Final assessment report](#) | European Commission.

Recently, four very similar cases in the Baltic Sea have tested the resilience of undersea infrastructure. The Balticconnector gas pipeline between Finland and Estonia and the EE-S1 data cable were damaged on 7 November 2023. The C-Lion1 cable between Finland and Germany was cut on 18 November 2024. The Estlink 2 electricity cable, together with four data cables, was damaged on 25 December 2024 between Finland and Estonia. An undersea fibre optic cable between Latvia and Sweden was damaged on 26 January 2025. None of these incidents caused significant disruptions to the security of supply, or relevant societal harm, indicating that the resilience of gas and communication infrastructure in the Baltic Sea is already high.

The incidents were all very similar: a ship with complex ownership structures damaged undersea cables or pipelines in a seemingly lawful manner by dragging an anchor along the seabed while sailing in international waters. Since anchors typically have safety mechanisms that prevent accidental drops, and dragging should be noticeable, it is highly likely that the damage was either intentional, or due to severe negligence. Presuming that physical damage was indeed the objective behind the intentional acts, it means that resilience alone has not served as a sufficient deterrent.

For this reason, the affected states, with support from the EU and NATO, are urgently seeking to improve their *deterrence by punishment*. They need to find more ways to improve accountability and, if need be, to impose costs on the actors behind the incidents. This includes the ships themselves, their captains, crew, owners, flag states, port states and authorities, as well as state actors using the ships as proxies for hybrid interference.

This is not an easy task. While responsibility issues are relatively clear once damage has been

caused, the competences of coastal state authorities to pursue and investigate a suspected vessel are limited to territorial waters or cooperation with the flag state – which, in cases of intentional damage, is typically nonexistent. Even with proper investigations, proving the intentionality of the action is difficult, and attributing the act to a state actor even harder. This makes this particular *modus operandi* a highly effective means of hybrid interference.

This Briefing Paper focuses on the challenges the EU and NATO face in improving their deterrence by punishment. While the four discussed incidents are relevant, they are only part of a much wider context of hybrid interference in the Baltic Sea region. Even when focusing solely on maritime security, it is necessary to consider the set of challenges posed by the use of the so-called shadow fleet, which not only circumvents existing sanctions against Russia, but also poses significant risks to undersea infrastructure and the environment in the shallow and complex waters of the Baltic Sea.

There is no single solution to the challenge of insufficient deterrence. Hence, a more strategic approach is needed, using the full spectrum of smaller measures, including those outside traditional security and defence policy frameworks. For instance, the EU could use its economic and trade policy instruments, as well as regulations on maritime transport and movement, to encourage flag states and private companies to assume their responsibilities.

### Military responses and their limitations

One of the responses to the recent incidents has been an increased NATO maritime presence. For instance, after the December 2024 case, the Alliance decided to “maintain vigilance, increase situational awareness, and deter future incidents”,<sup>4</sup> which in practical terms entailed the immediate deployment of a couple of patrol vessels to the area and enhancing

<sup>4</sup> [NATO - News: NATO to enhance military presence in the Baltic Sea, 30 Dec 2024.](#)

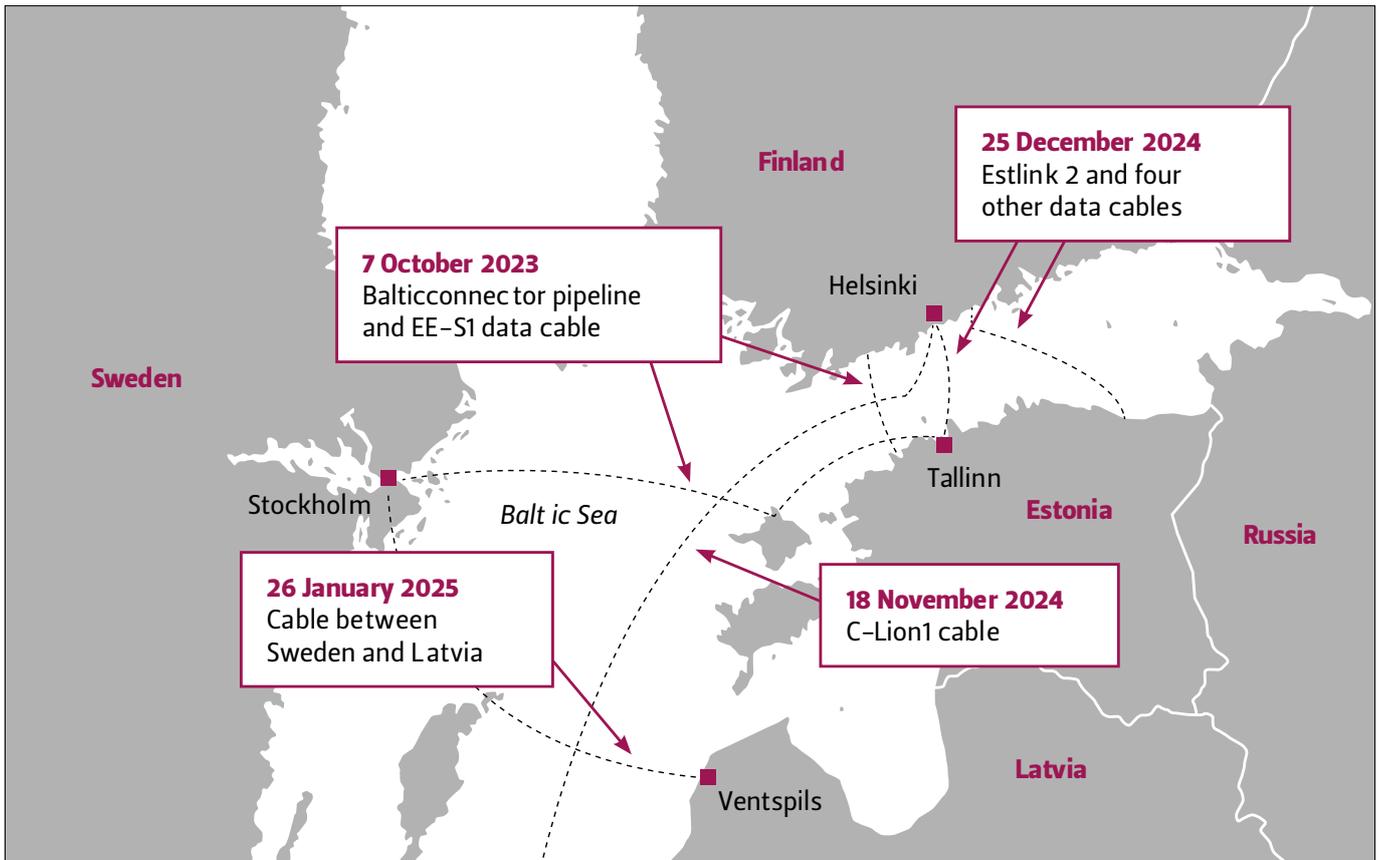


Figure 1. Map of the Baltic Sea region and damaged undersea cables and pipelines between 2023-2025

aerial and spatial surveillance. While such measures are standard NATO protocol in similar situations, the presence was further strengthened when several heads of state, at a Summit of Baltic Sea Allies on 14 January 2025, launched the “Baltic Sentry” operation, consisting of additional frigates, patrol aircraft and vessels, as well as unmanned surface vessels.

## **“There is a reason why civilian vessels are used to cause the damage instead of military submarines.”**

The visible presence of warships in the Baltic Sea serves as an efficient deterrent against deliberate pipeline sabotage, and undoubtedly prevents further escalation of hostile actions. However, it is not a long-term solution. Meanwhile, when sabotage is carried out using civilian ships in a seemingly innocent manner, military vessels can only support the coast guard – who is responsible for law enforcement in cases where civilian vessels cause damage, whether accidental or intentional – in pursuing and stopping the suspected ships.

If the Baltic Sea incidents are indeed hybrid actions by state actors, there is a reason why civilian vessels are used to cause the damage instead of military submarines. The state actors behind the sabotage seek to inflict harm without escalating the situation into an open military confrontation. Since the aim of deterrence by punishment is to prevent but not escalate, non-military means may prove more efficient in countering hybrid interference.

In addition to increased presence, the military has other tools that can make a difference, particularly regarding the surveillance and situational awareness of undersea infrastructure. For example, the UK-led Joint Expeditionary Force (JEF) will use the Nordic Warden system to enhance surveillance in the proximity of critical undersea infrastructure through the use of the Automatic Identification System and artificial intelligence tools.<sup>5</sup> This is an important example of how new and emerging technologies, along with better information sharing, can also be used in the context of hybrid threats.

<sup>5</sup> [Joint Expeditionary Force activates uk-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet - GOV.UK.](#)

In this context, it is useful to note that critical infrastructure protection is a field where state interests – ensuring security of supply and protecting sovereignty – align fully with the interests of private companies, which own most of the cables and pipelines. Hence, improving information sharing on security breaches should be relatively straightforward, as should finding financial solutions for developing better surveillance tools and instruments both below and above the surface.

To speed up the capability development, Baltic Sea states that are members of both the EU and NATO could also consider advancing these initiatives more rapidly by enhancing regional cooperation and investing further in the region’s security. For instance, the shadow fleet is a shared problem linked to hybrid interference and environmental security, and its risks can only be mitigated through collective action.

## **Pursuing capabilities**

When damage to critical undersea infrastructure is caused by a civilian ship, it is primarily a law enforcement issue. This means that the responsibility for pursuing the suspected vessel lies with the police, border guards, and coast guards of the affected states. Military capabilities, along with the relevant international cooperation frameworks, should support the process with all available means. For instance, both military and civilian satellite and intelligence services can rapidly provide data on maritime movements at the incident site.

This was also the case with the four incidents under discussion: the affected states and their law enforcement authorities led the response, and cooperation between the Baltic Sea EU member states and NATO allies functioned effectively. Additionally, the affected states actively engaged with the EU and NATO, both of which are able to support investigations with their maritime, air, space and intelligence services, as well as diplomatically, if needed.

In the recent incidents, the identification of the suspected vessels was relatively swift, and a steep learning curve can also be observed in the speed of the response by law enforcement authorities and their international cooperation. For example, *Newnew Polar Bear*, the vessel linked to the Balticconnector damage in 2023, managed to sail away from the Baltic Sea. In contrast, *Yi Peng 3*, suspected

in the November 2024 incident, was stopped in the Kattegat, at the exit of the Baltic Sea. *Eagle S* and *Vezhen*, suspected in the December 2024 and January 2025 incidents respectively, were intercepted within a few hours in the vicinity of the affected states. Due to Chinese cooperation, the Finnish authorities were eventually allowed to investigate *Newnew Polar Bear* in China. *Yi Peng 3* was permitted to continue its passage in the absence of firm evidence against it, while *Eagle S* and *Vezhen* remain under investigation at the time of writing.

A proper criminal investigation, including the examination of financial transactions and the interrogation of the captain and crew, is essential for finding evidence of possible state involvement, such as bribery by intelligence operators. This has only been possible in the last two cases, but it may nevertheless be difficult to prove that the damage was intentional. This makes it difficult to attribute the actions to any state actor, which is essential for implementing most restrictive measures such as sanctions.

Despite the evident improvement in pursuing and investigating the suspected ships, there is still no agreed operational protocol on how the Baltic Sea states should cooperate in such cases. Moreover, in some countries, even internal competences vary significantly, leaving room for improvement.

The existing legal framework contains loopholes that, to some extent, allow those responsible for either accidental or intentional damage to simply sail away. Meanwhile, there is little that the law-enforcement authorities can do without the support of the flag state authorities. However, changing the current laws would likely be difficult and slow, even with strong political will and a coalition of strong allies. The focus therefore remains on operating as effectively as possible within the existing legal frameworks.

### **Manoeuvring within the existing legal frameworks**

The rights and rules of navigation are established in the United Nations Convention on the Law of the Sea (UNCLOS), including the conditions under which coastal states may pursue vessels. UNCLOS allows coastal states to stop and search vessels engaged in “innocent passage” in territorial waters if there is reasonable suspicion that they are involved in illegal activity. This was the case with *Eagle S* in December

2024, when the Finnish authorities managed to direct the tanker into Finnish territorial waters, allowing them to board and detain the vessel for examination. However, the situation becomes more complicated if the suspected vessel remains in international waters, as authorization from the ship’s flag state is required to stop and board the ship.

In cases of hybrid interference, the flag state is either complicit in the act and unwilling to cooperate, or the ship and its crew are being used as proxies by another state or non-state actor. In both situations, it is up to the flag state to allow or conduct the necessary investigations.

Even in cases of unintentional damage or ships being used as proxies, flag states often prioritize protecting their sovereignty when possible, and may prefer to lead the investigation themselves. This may or may not yield results, depending on how thoroughly investigations are conducted. For example, in the Balticconnector case in 2023, China was cooperative with the Finnish authorities but rejected Sweden’s request to board and investigate the ship involved in the C-Lion damage in 2024. In the December 2024 case, the flag state of the suspected vessel, Cook Islands, has been cooperating with the Finnish authorities, while in the January 2025 case, Sweden was able to initiate a criminal investigation into the ship sailing under the Maltese flag.

**“It is also necessary to consider the possibility that the primary aim of the sabotage may not have been the critical infrastructure itself.”**

Given that UNCLOS allows “innocent passage” in territorial waters and any type of transit in international waters, there is significant leeway for hybrid interference, and for getting away with it. For this reason, armies of lawyers and legal experts in the Baltic Sea countries, the EU and NATO are now looking at the convention to find ways to interpret the current text in a manner that would make it easier to stop and inspect ships responsible for damage, intentional or not. The concept of “innocent passage” will certainly come under scrutiny, along with the use of straits – which is particularly relevant in the Baltic Sea, where all maritime transit in and out of the region passes through the strait between Denmark and Sweden.

Nevertheless, any potential changes to international law should be considered in a global context. Countries with large merchant fleets, even those on the Baltic Sea coast, such as Denmark and Germany, seem unwilling to modify restrictions on international navigation or to expand coastal states' authority to stop and investigate ships in international waters. There is also a risk that revisiting the law in the current context of increasing global competition might not lead to better outcomes from the perspective of economic freedom.

In this context it is also necessary to consider the possibility that the primary aim of the sabotage may not have been the critical infrastructure itself. As noted, the energy and communication networks have proven resilient, and the damage has been limited. Another possibility is that the aim of the sabotage is to lure the affected states into a so-called *reflexive trap* regarding the rules-based global order. In other words, by provoking with sabotage, the state actor behind the action may hope that the targeted countries would bypass UNCLOS and act outside international regulations by stopping and boarding suspected ships in international waters. If the Baltic Sea countries – many of which are strong defenders of the rules-based global order – were to act outside the rule of law for their own short-term interests, it would set a dangerous precedent that could undermine that very order. Many authoritarian states would likely welcome this, since it would justify closing strategic straits and limiting the use of international waters for strategic rivals.

### **Sabotage as acts of terrorism**

In the context of hybrid threats, some countries, such as Lithuania, have often investigated such cases under terrorism legislation. The state prosecutor in Finland also considered this approach in relation to the December 2024 damage to communication cables. The question is whether sabotage can be considered act of terrorism and, if so, whether it would provide any added value in terms of legal authority over suspected vessels.

All EU countries have incorporated Directive (EU) 2017/541 on Combatting Terrorism into their national legislation. According to the directive, offences “causing extensive destruction to [...] an infrastructure facility, including an information system”, with the aim of “seriously destabilising or

destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation” can be considered acts of terrorism. Therefore, depending on how “fundamental” the structures are deemed, the sabotage could qualify as an act of terrorism – although this interpretation may differ significantly from how the wider public typically understands terrorism.

Classifying sabotage as an act of terrorism could add value in terms of deterrence. In some countries, the police may have wider competences when investigating terrorism-related crimes compared to other criminal offences. In the same vein, penalties for terrorism offences are typically harsher, meaning that they could enhance deterrence by punishment. However, these competences are only relevant if the state has the authority to stop and investigate the suspected vessel and its crew, meaning that simply classifying sabotage as terrorism does not resolve the issues regarding UNCLOS.

### **Use of restrictive measures**

One of the strongest tools that can be used against malicious actors below the threshold of military action is the use of restrictive measures, such as sanctions, travel bans, and asset freezes. These measures would serve as useful additional leverage against those states that allow ships under their flags to cause damage in the Baltic Sea, pressuring them to allow proper criminal investigations. In this regard, the EU should take the lead, since the cases at hand impact the common European critical infrastructure.

Since autumn 2024, the EU has had a sanctions regime against Russian destabilizing activities targeting the EU and its member states, designed to address a wide range of hybrid activities. However, this regime currently applies only to Russia and its possible proxies. Without clear evidence pointing to Russian state involvement, it cannot be used. To make the regime more flexible and applicable to all cases involving hybrid interference, it would make sense for the EU to convert this regime into an actor-agnostic framework. This would allow sanctions to be imposed on any state actor involved, not just Russia. Such an approach would enable the EU to impose economic costs on all hybrid actors and their proxies, including vessel owners, flag states, as well as relevant port states, if there is any indication that the damage has been intentional.

In cases where the sabotage is investigated and ruled an act of terrorism, the EU also has an existing sanctions regime on terrorism, which could, in principle, be applied to any actors involved. However, this regime is primarily aimed at non-state actors, typically those recognized as terrorist organizations. Nevertheless, the EU has quick and easy options to use sanctions, also in the context of the sabotages, if there is enough political will in the member states.

### **Asymmetric response options**

The four cases discussed clearly demonstrate the tendency to seek symmetric responses within the affected domains: maritime incidents are met with increased maritime presence and surveillance, or addressed through interpretations of UNCLOS. However, this is not necessarily the domain where the targeted country, the EU or NATO has the most effective response options. To develop responses with more weight, it is necessary to explore options in other domains.

### **“Challenges in existing international law make it difficult to hold malicious state and non-state actors accountable for their actions.”**

For instance, the EU wields significant soft power through its diplomatic clout, economic leverage, and ability to set international rules and regulations. It could seek ways to better regulate shipping in European waters, for example by imposing insurance and environmental requirements. This would restrict the shadow fleet, which has been linked to sabotage in the Baltic Sea. The same could be applied to commerce in Europe when dealing with murky companies and ship owners, while visa regimes could be used to exert pressure on distant flag states that refuse to cooperate with investigations.

Even if the individual measures alone would not provide sufficient deterrence by punishment, their coherent and coordinated use would raise the costs of destabilizing acts to such an extent that malicious actors, and especially their proxies, would think twice before dropping anchor.

## **Conclusions**

Looking at the undersea incidents from the wider perspective of ongoing hybrid activities, they are just one part of a much bigger game in which malicious actors – largely well-known states – are ready to weaponize almost anything to destabilize their adversaries. This includes not only attacks on critical infrastructure but also electoral manipulation, cyberattacks, and the instrumentalization of migrants. However, the targeted countries, the EU and NATO have not yet exhausted all their options for using deterrence by punishment, leaving adversaries with the initiative while the EU and NATO remain merely reactive.

Challenges in existing international law make it difficult to hold malicious state and non-state actors accountable for their actions, be they intentional or due to negligence. However, many options remain within the current frameworks, depending on the political will to use them. At a minimum, affected states should agree on common operational protocols and cross-border cooperation, including information exchange, in cases like the Baltic Sea incidents.

NATO plays an important role in preventing the escalation of malicious activities, and can contribute significantly to the development and improvement of current and future capabilities for surveillance and detection. These capabilities are relevant not only for defence, but also for law enforcement in cases such as the sabotage in the Baltic Sea. In this regard, civilian-military and public-private cooperation is key.

However, since hybrid interference is designed to remain below the threshold of open military confrontation, there should also be ways to impose costs at that level. This is where the EU could distinguish itself through its soft power and influence on global norms and regulations. A low-hanging fruit would be to impose sanctions on those responsible for the damage, but the EU also has powerful trade measures at its disposal that could serve as leverage against relevant flag states. Additionally, the EU could tighten regulations on insurance requirements and technical standards for ships navigating European waters, thereby contributing to overall deterrence.

While none of these measures alone is sufficient to provide more credible deterrence by punishment, when applied coherently and collectively, they significantly raise the costs for any would-be hybrid actor or its proxies. ●

BRIEFING  
PAPER  
**404**  
February 2025

ISBN 978-951-769-819-1

ISSN 1795-8059

Language editing: Lynn Nikkanen

Graphic design: Joonas Juutilainen

Cover photo: NATO, CC BY-NC-ND 2.0, cropped from the original

**FIIA**  
FINNISH  
INSTITUTE OF  
INTERNATIONAL  
AFFAIRS

**Arkadiankatu 23 b**  
**POB 425 / 00101 Helsinki**  
**Telephone +358 (0)9 432 7799**  
**[www.fia.fi](http://www.fia.fi)**



The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decision-making and public debate both nationally and internationally.

All manuscripts are reviewed by at least two other experts in the field to ensure the high quality of the publications. In addition, publications undergo professional language checking and editing. The responsibility for the views expressed ultimately rests with the authors.