ieee.es
Instituto Español de Estudios Estratégicos

Research
Paper

03/2026 mayo de 2026

Marta Molina Urosa, Javier Lafuente Capó, Manuel Lopera Rodríguez, Laura Ruiz Sancho, Gerard Terrés Pueyo, Pablo García Hernández

Critical Infrastructure in the Context of Hybrid Warfare: Submarine Cables, Geopolitical Competition, and Structural Vulnerability in the Baltic Sea

[Visit the website](#) [Subscribe to the E-NEWSLETTER](#)

Critical Infrastructure in the Context of Hybrid Warfare: Submarine Cables, Geopolitical Competition, and Structural Vulnerability in the Baltic Sea

Abstract:

This article examines the growing vulnerability of submarine cables in the Baltic Sea within the context of hybrid warfare and intensifying geopolitical competition. It argues that the physical characteristics of these infrastructures, combined with a fragmented legal framework marked by attribution challenges and normative ambiguities, create favourable conditions for grey-zone operations. In an increasingly contested regional environment, submarine cables have become a strategic vector for disruptive activities below the threshold of armed conflict.

The article develops a conceptual framework to analyse the strategic relevance of submarine cables and assesses the geopolitical dynamics and structural conditions that heighten their vulnerability in the Baltic Sea. It also evaluates the responses of the European Union and NATO, identifying recent initiatives alongside persistent limitations in their capacity to deter, attribute and respond to hybrid threats. Incidents recorded between 2022 and 2025 suggest that the Baltic Sea is increasingly functioning as a testing ground for hybrid tactics.

Keywords:

Submarine cables, geopolitics, hybrid warfare, Russia, China, critical infrastructure.

How to cite this document:

MOLINA UROSA, Marta *et al. Critical Infrastructure in the Context of Hybrid Warfare: Submarine Cables, Geopolitical Competition, and Structural Vulnerability in the Baltic Sea*. IEEE Research Paper 03/2026. IEEE web link and/or bie³link (accessed day/month/year)

Marta Molina Urosa, Javier Lafuente Capó, Manuel Lopera Rodríguez, Laura Ruiz Sancho, Gerard Terrés Pueyo, Pablo García Hernández

In a deeply interconnected world, submarine cables form the backbone of the global telecommunications economy: over 99% of international data traffic and nearly 90% of communications between Europe and the United States depend on this physical network of approximately 500 cables stretching over 1.7 million kilometres[1] [2] .

These systems underpin government communications, financial transactions, cloud services, supply chains and access to information for billions of people[3] .

Their status as critical infrastructure is reflected in the scale of their vulnerability: between 150 and 200 faults are recorded worldwide each year. Furthermore, in 2023 the International Cable Protection Committee (ICPC) documented more than 200 repairs, equivalent to more than three incidents per week[4].

Although much of this damage is attributed to accidental causes—primarily anchor drags, navigational errors or fishing activities[5] —the line between accident and sabotage has become increasingly blurred.

This ambiguity stems, in part, from the very nature of the maritime domain. The law of the sea, whilst providing a basic framework, proves insufficient to guarantee the protection and attribution of liability regarding infrastructure that is, in many cases, outside the direct criminal jurisdiction of coastal states[6].

The ability to disable Automatic Identification Systems (AIS) — systems that transmit the position and identity of vessels to ensure safety and facilitate tracking[7] —, the use of flags

[1] INTERNATIONAL TELECOMMUNICATION UNION. 'Submarine Cable Resilience', *ITU*. 2024. Available at: https://www.itu.int/digital-resilience/submarine-cables/
Note: All hyperlinks are active as of 9 April 2026.
[2] LOIK, R. 'Undersea hybrid threats in strategic competition: The emerging domain of NATO–EU defence cooperation', *Journal on Baltic Security*, 10(2). 2024, pp. 1–25. https://doi.org/10.57767/jobs_2024_008
[3] INTERNATIONAL TELECOMMUNICATION UNION. *Op. cit.*
[4] INTERNATIONAL TELECOMMUNICATION UNION. 'Press Release: International summit outlines steps to improve resilience of submarine telecommunications cables worldwide', *ITU.* 2024. Available at: https://www.itu.int:443/en/mediacentre/Pages/PR-2025-02-27-submarine-cables-summit-nigeria.aspx
[5] Ibid.
[6] O'RIORDAN, K. 'Geopolitics of Baltic subsea infrastructure (Map 11)', *Brussels Institute for Geopolitics*. 2025. Available at: https://big-europe.eu/publications/2025-04-11-geopolitics-of-baltic-subsea-infrastructure
[7] CALDWELL, J. 'Security or safety: what is AIS really for?', *CIMSEC*. 19 May 2025. Available at: https://cimsec.org/security-or-safety-what-is-ais-really-for/

of convenience, or the absence of witnesses, make the underwater environment a fertile ground for grey-zone operations and the resulting plausible deniability[8].

Thus, both civilian vessels and state actors can operate under conditions of opacity that hinders the clarification of incidents and offers opportunities for the execution of hybrid actions that are difficult to trace.

Since 2022, this structural vulnerability has taken on an additional geopolitical dimension. The war in Ukraine transformed the Baltic Sea —traditionally perceived as a stable and interdependent sea— into a space of strategic confrontation between the Euro-Atlantic bloc and revisionist powers[9] [10].

Finland and Sweden's accession to NATO consolidated the allied perimeter in the basin, whilst the Russian coast and the Kaliningrad enclave retain their role as a platform for military projection[11] [12].

In this context, the Baltic Sea is of fundamental importance for telecommunications, military interoperability, energy security and European economic resilience.

This strategic centrality is largely explained by the configuration of its seabed, which hosts a particularly dense network of submarine cables connecting European Union (EU) and North Atlantic Treaty Organisation (NATO) states to one another and to Russia, particularly the Kaliningrad enclave[13] [14].

This infrastructure is managed by a complex network of European, Chinese, Russian and American owners and operators, reflecting both a deep interdependence and, at the same time, the strategic tensions inherent in the region[15].

[8] BERNABÉ, P. *et al.* 'Detecting Intentional AIS Shutdown in Open Sea Maritime Surveillance Using Self-Supervised Deep Learning', *IEEE Transactions on Intelligent Transportation Systems*, 25(2). 2024, pp. 1166–1177. Available at: https://doi.org/10.1109/TITS.2023.3322690
[9] CHARALAMBIDES, Y. 'A Russian revisionist strategy on the rise?', *Taylor & Francis*, *Strategic Analysis*, 46(2). 2022, pp. 141–156. Available at: https://doi.org/10.1080/09700161.2022.2076303
[10] LOIK. *Op. cit.*
[11] KALEDIN, N. V. and ELATSKOV, A. V. 'Geopolitical regionalisation of the Baltic area: The essence and historical dynamics', *Baltic Region*, 16(1). 2024, pp. 141–158. Available at: https://doi.org/10.5922/2079-8555-2024-1-8
[12] SWISTEK, G. and PAUL, M. 'Geopolitics in the Baltic Sea region: The "Zeitenwende" in the context of critical maritime infrastructure, escalation threats and the German willingness to lead' (SWP Comment 2023/C 09), *Stiftung Wissenschaft und Politik* (SWP). 2023. https://doi.org/10.18449/2023C09
[13] KALEDIN, N. V. and ELATSKOV, A. V. *Op. cit.*
[14] SWISTEK, G. and PAUL, M. *Op. cit.*
[15] O'RIORDAN. *Op. cit.*

It is worth noting that these cables are privately owned, which poses significant challenges in terms of incident attribution, repair and strategic resilience.

In this context, this article aims to analyse how the convergence of physical, legal and geopolitical factors in the Baltic Sea makes submarine cables a key vector for hybrid warfare, against which the response capabilities of the European Union and NATO remain insufficient.

It thus examines the structural limitations faced by both organisations in terms of protection, attribution and response, and also assesses the strategic evolution of the region and actions in the so-called grey zone.

To this end, the study is structured into five sections: firstly, it establishes the conceptual framework regarding hybrid warfare, the grey zone and plausible deniability; secondly, it reviews recent incidents and the evolution of the Baltic environment since 2022; thirdly, it analyses the factors explaining the vulnerability of submarine infrastructure; fourthly, the challenges these dynamics pose for the EU and NATO are examined, particularly in terms of surveillance, attribution and digital sovereignty; and, finally, Western responses and the limits of collective action are addressed, with a view to assessing institutional adaptation in an environment marked by strategic ambiguity and growing geopolitical competition.

Conceptual framework: hybrid warfare, the grey zone and plausible deniability

To understand the analytical basis of this work, it is necessary to address the concept of hybrid warfare, a concept established by Frank Hoffman (2007). Hoffman characterises it as ‘different modes of warfare, including conventional modes, irregular tactics and formations, as well as terrorist acts, including indiscriminate violence and public disorder’[16] .

NATO defines hybrid warfare as ‘a broad, complex and adaptive combination of conventional and non-conventional means, as well as military, paramilitary and civilian

[16] HOFFMAN, F. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, 2007. Available at: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

measures, both overt and covert, employed in an integrated manner by states and non-state actors to achieve their objectives'[17] .

Over time, this logic has resulted in covert, ambiguous and uncertain actions, the nature of which makes it difficult to clearly attribute responsibility.

In this context, the 'grey zone' emerges, understood as a space of confrontation characterised by 'aggressive yet deliberately calculated coercive actions, designed to remain below the threshold that might trigger an overt military response'[18] .

The effectiveness of these actions lies in their ambiguity: neither the perpetrator nor their intentions can be attributed with certainty. This lack of attribution erodes states' capacity to respond, by limiting the use of legal tools and hindering the mobilisation of international consensus[19] .

The attribution—that is, the conclusive identification of the party responsible for a hostile act—is, therefore, a central element in this type of scenario. It is not merely a technical matter, but also a political and strategic one: attribution makes it possible to convince allies, to communicate to the public the existence of an adversary and to lend legitimacy to any retaliatory or deterrence.

In the absence of clear attribution, strategic ambiguity becomes a weapon in and of itself. When the probability of being identified is low, aggressors reap high rewards with a reduced risk of retaliation.

Added to this ambiguity is a key component of contemporary conflicts: plausible deniability (plausible denial). As Rid and Buchanan (2015), this concept allows state or non-state actors to deny their involvement in hostile actions.

The concept of plausible deniability takes on particular significance in environments where the collection, traceability, and verification of evidence are especially complex,

[17] NORTH ATLANTIC TREATY ORGANISATION. *Final Declaration of the Warsaw Summit* (para. 72). NATO, 9 July 2016. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm
[18] MAZARR, M. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Books, Monographs & Collaborative Studies, 2015. Available at: https://press.armywarcollege.edu/monographs/428
[19] Ibid.

such as the maritime sector and, specifically, the sector related to subsea infrastructure and communications cables[20] [21].

So far, plausible deniability has been the main strategic advantage of the actors who have carried out hybrid operations against critical infrastructure of this nature[22] [23].

In this context, the concept of maritime accidents becomes relevant, which encompasses unintentional incidents such as the accidental dragging of anchors, navigational errors, interference resulting from trawling, or damage caused by adverse weather conditions[24] [25] [26].

Although these events are part of the normal operations of the maritime environment, in the current strategic context, this category has been exploited by state and non-state actors to conceal hostile actions against critical infrastructure[27].

The possibility of presenting an act of sabotage as an accident reinforces plausible deniability and complicates attribution, thereby reinforcing the logic of the grey area.

Furthermore, these incidents allow for indirect interference in the internal politics of EU and NATO member states through such as the use of vessels with identification systems switched off[28].

Strategic ambiguity, reinforced by narratives that justify or downplay the harm caused, benefits both the alleged perpetrator —by maintaining a plausible denial— as well as, on some occasions, the affected state, which may choose not to publicly challenge the accidental version in order to avoid escalation and preserve the status quo[29] [30].

---

[20] BUEGER, C. and LIEBETRAU, T. 'Critical maritime infrastructure protection: What's the trouble?', *Marine Policy*, 155. 2023, 105772. Available at: https://doi.org/10.1016/j.marpol.2023.105772
[21] CONTE DE LOS RÍOS, A. *New European Maritime Safety Strategy 2023*. Opinion Paper IEEE 104/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO104_2023_AUGCON_Estrategia_ENG.pdf
[22] RID, T. and BUCHANAN, B. *Op. cit.*
[23] OGRYZKO, L. and RIZZI, A. *Op. cit.*
[24] CLAKE, M. *Submarine Cable Protection and the Environment*. An Update from the ICPC (Issue 6). International Cable Protection Committee, ICPC, 2023. Available at: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_November_2025.pdf
[25] International Telecommunication Union. *Op. cit.*
[26] BUEGER, C. 'What is maritime security?', *Marine Policy*, 53. 2015, pp. 159–164. Available at: https://doi.org/10.1016/j.marpol.2014.12.005
[27] INSIKT GROUP. 'Global threats to submarine cable infrastructure', *Recorded Future*. 2023. Available at: https://www.recordedfuture.com/resources/russian-undersea-capabilities

[28] OGRYZKO, L. and RIZZI, A. *Op. cit.*
[29] REICHBORN-KJENNERUD, E. and CULLEN, P. *What is Hybrid Warfare?* Norwegian Institute of International Affairs Policy Brief 1/2016. https://nva.sikt.no/registration/0198cc7d0bf6-4f24ef7c-9045-401d-87de-46da2f39e4da
[30] OGRYZKO, L. and RIZZI, A. *Op. cit.*

In short, the interplay between hybrid warfare, the grey zone, plausible deniability, the difficulties of attribution and the normalisation of maritime accidents create a strategic environment particularly conducive to covert coercion in the submarine domain, as illustrated by the case of the Baltic Sea.

Recent incidents and strategic developments in the Baltic region

The Russian invasion of Ukraine in 2022 and the accession of Finland and Sweden to NATO transformed the Baltic Sea from a relatively unstable area into a front line of strategic confrontation. This new configuration of the Baltic as a 'NATO lake'[31] [32] [33], which will be detailed later, has increased the geopolitical significance of incidents in the region.

Since 2023, damage recorded to submarine cables—particularly around the Balticconnector and on links between Finland, Estonia and Sweden—has highlighted a growing vulnerability. Although initially attributed to accidents, the repetition of patterns and their spatial concentration have heightened suspicions of covert intent[34] [35] [36] .

This trend is also reflected in the available data. Although much of it is classified, the aforementioned 200 annual incidents are significant[37] . Since 2023, there has thus been a shift from isolated failures to potentially coordinated damage, as demonstrated by the most significant incidents detailed below.

- October 2023: the container ship NewNew Polar Bear (flying the Chinese flag) damaged two cables and the Balticconnector due to an anchor dragging incident. Finland and Sweden described the incident as an accident resulting from an

[31] CHARALAMBIDES, Y. *Op. cit.*
[32] LOIK. *Op. cit.*
[33] KALEDIN, N. V. and ELATSKOV, A. V. *Op. cit.*
[34] BRAW, E. 'How the Baltic Sea nations have tackled suspicious cable cuts', *Atlantic Council*. 26 November 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/
[35] CODREANU, M. C. 'Crossing the line: Severing undersea internet cables in geopolitical hotspots', *Policy Brief* No. 76. New Strategy Center, 2025. https://www.newstrategycenter.ro/wp-content/uploads/2025/06/Codreanu_PB76_EN-1.pdf
[36] *THE ECONOMIST*. 'Who is sabotaging underwater infrastructure in the Baltic Sea?'. 22 October 2023. https://www.economist.com/europe/2023/10/22/who-is-sabotaging-underwater-infrastructure-in-the-baltic-sea
[37] INTERNATIONAL TELECOMMUNICATION UNION. *Op. cit.*

operational error or negligence linked to the poor condition of the vessel, although suspicions of deliberate action persisted, though these could not be proven[38] .

- December 2024: the oil tanker *Eagle S* (Cook Islands-flagged), linked to the Russian *shadow fleet*, severed five cables and the Estlink 2 interconnector. The 90 km anchor drag suggested a pattern consistent with gross negligence; however, the location of the incident within the exclusive economic zone (EEZ) limited the scope of Finnish jurisdiction[39] [40] . The case, currently under appeal by the Finnish prosecution, has been interpreted as a paradigmatic episode of hybrid warfare[41] .
- January 2025: Sweden seized the vessel Vezhen (flying the Maltese flag and with a predominantly Bulgarian crew) after it damaged a cable between Latvia and Gotland. Although the incident was ultimately attributed to human error, it contributed to reinforcing the perception of risk in the region[42] .

The case of Estlink 2 is particularly significant. Its repair took seven months, in the middle of the Baltic winter, and investigations revealed the presence of counter-surveillance equipment, as well as an anchor mark coinciding with the Eagle S's trajectory, which reinforced the theory of sabotage[43] [44] . This episode prompted an intensification of surveillance cooperation between NATO and the Baltic states[45] .

[38] BESCH, S. and BROWN, E. 'Securing Europe's Subsea Data Cables', *Carnegie Endowment for International Peace*. 16 December 2024. Available at: https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables

[39] LOTT, A. 'Maritime Security in the Baltic and Japanese Straits From the Perspective of EEZ Corridors', *Ocean Development & International Law*, 54(3). 2023, pp. 327–348. Available at: https://doi.org/10.1080/00908320.2023.2265301

[40] BRAYANT, M. and *correspondent,* M. B. N. 'Finland charges tanker crew members with sabotage of undersea cables', *The Guardian*. 11 August 2025. https://www.theguardian.com/world/2025/aug/11/finland-accuses-tanker-crew-sabotage-undersea-cables-anchor

[41] SWISSINFO. "Finland accuses three oil tanker sailors of sabotaging cables in the Baltic Sea", *SWI swissinfo.ch*. 11 August 2025. https://www.swissinfo.ch/spa/finlandia-acusa-a-tres-marineros-de-un-petrolero-por-sabotear-cables-en-el-mar-báltico/89816031

[42] AHLANDER, J. and RINGSTROM, A. "Swedish authorities board ship seized over Baltic Sea cable breach", *Reuters*. 27 January 2025. https://www.reuters.com/world/europe/swedish-authorities-board-ship-seized-over-baltic-sea-cable-breach-2025-01-27/

[43] 20MINUTOS INTERNATIONAL. "Did a Chinese ship cut the Baltic cables? Investigators are looking into the route of the cargo ship Yi Peng 3 and whether it was responsible for the sabotage." 22 November 2024. https://www.20minutos.es/noticia/5656513/0/suecia-dinamarca-investigan-buque-chino-causo-doble-sabotaje-baltico/

[44] QIU, W. "Finland Charges Russian-Linked Ship Officers Over Baltic Sea Cable Sabotage", *Submarine Cable Networks*. 13 August 2025. https://www.submarinenetworks.com/en/nv/insights/finland-charges-russian-linked-ship-officers-over-baltic-sea-cable-sabotage

[45] Ibid.

Although most documented incidents involve submarine cables, other strategic infrastructure has also been targeted. In particular, the Nord Stream 1 and Nord Stream 2 gas pipelines were sabotaged in September 2022.

Initial suspicions pointed to Russia, although the Kremlin denied this and cited the high economic value of the pipelines for its own interests[46] . The subsequent arrest in Germany of a Ukrainian citizen added complexity to the case and highlighted that the hybrid confrontation in the Baltic Sea is characterised by ambiguity, uncertain attribution and a plurality of actors[47], which poses a challenge for deterrence and collective response.

[46] SOLDI, G. *et al*. 'Monitoring of underwater critical infrastructures: The Nord Stream and other recent case studies', *Cornell University*. https://doi.org/10.48550/arXiv.2302.01817

[47] KOPER, A. 'Polish court says Ukrainian wanted in Nord Stream case must remain in custody', *Reuters*. 10 January 2025. https://www.reuters.com/world/europe/polish-court-says-ukrainian-wanted-nord-stream-case-must-remain-custody-2025-10-01/

Date	Infrastructure affected	Actor or vessel involved	Type of damage	Official conclusions / status of the investigation
Sept. 2022	**Nord Stream 1 and 2 gas pipelines**	Unidentified (various suspicions)	Underwater explosions	Perpetrators unconfirmed; initial suspicions pointed towards Russia, later towards possible Ukrainian actors; investigation still ongoing
Oct. 2023	**Balticconnector + 2 telecommunications cables**	NewNew Polar Bear (Chinese-flagged)	Anchor dragging	Deemed an accident by Sweden and Finland; no evidence of intent, though strong strategic suspicion
Dec. 2024	**Estlink 2 + 5 telecommunications cables**	Eagle S (Cook Islands, linked to *shadow fleet*)	Multiple cuts caused by anchor dragging	Evidence of a 90 km trail; Finland interprets as sabotage; jurisdictional limitations; case under appeal
Jan. 2025	**Latvia–Gotland cable**	Vezhen (Maltese flag)	Damage caused by dragging or improper manoeuvring	Investigated as possible sabotage; ultimately classified as an accident due to human error
2024–2025	**Estlink 2 (repair)**	—	Complex structural damage	Repair completed in August 2025; duration ~7 months due to technical and meteorological complexity

Table1 . Incidents in the Baltic Sea (2022–2025). Own compilation

Geopolitical factors in the Baltic Sea

The Baltic region can be understood as a geopolitical system centred on the Baltic Sea and the Danish straits, integrating maritime, coastal and terrestrial areas, as well as the main transport routes between ports and inland territories (*hinterlands)*[48] .

Illustration1 . The Baltic Sea region (Savitz & Winston, 2024)

This is an environment characterised by the overlap of multiple domains—maritime, geographical, economic and strategic—and by a large number of actors, including Nordic countries, Baltic states and Central European countries, both NATO members and non-members. This diversity shapes a region in which relations of cooperation and conflict coexist at different scales and in different spheres[49] [50] .

From a geopolitical perspective, the Baltic Sea has established itself as a bipolar enclave, situated at the interface between the Euro-Atlantic and Eurasian subsystems.

This dynamic translates into a growing confrontation between a Baltic-Euro-Atlantic bloc—comprising EU and NATO member states—and a Baltic-Eurasian bloc, centred on Russia and China[51] .

Within this broader framework, the Baltic maritime region has emerged as a focal point of geopolitical interest and conflict due to a combination of three factors: (i) its almost established status as a 'NATO lake'; (ii) Russia's militarised presence in Kaliningrad; and (iii) the existence of a dense network of critical infrastructure—in particular submarine telecommunications cables —linking EU and Alliance states to one another, and also connecting them to Russia[52] [53] [54] .

[48] KALEDIN, N. V. and ELATSKOV, A. V. *Op. cit.*
[49] Ibid.
[50] SWISTEK, G. and PAUL, M. *Op. cit.*
[51] CHARALAMBIDES, Y. *Op. cit.*
[52] BUEGER, C., LIEBETRAU, T. & FRANKEN, J. *Security threats to undersea communications cables and infrastructure – Consequences for the EU* (PE 702.557). European Parliamentary Research Service, 2022. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2022)702557
[53] LOIK. *Op. cit.*
[54] O'RIORDAN. *Op. cit.*

From a Euro-Atlantic perspective, the accession of Finland (2023) and Sweden (2024) to NATO has decisively reinforced the perception of the Baltic as a 'NATO lake'[55] [56] [57], by placing virtually its entire coastline under the Alliance's umbrella. For the European Union, this region is also strategic for the cohesion of the digital single market, given that undersea cables ensure connectivity between Member States and the Baltic countries, as well as the security of trade and energy routes[58].

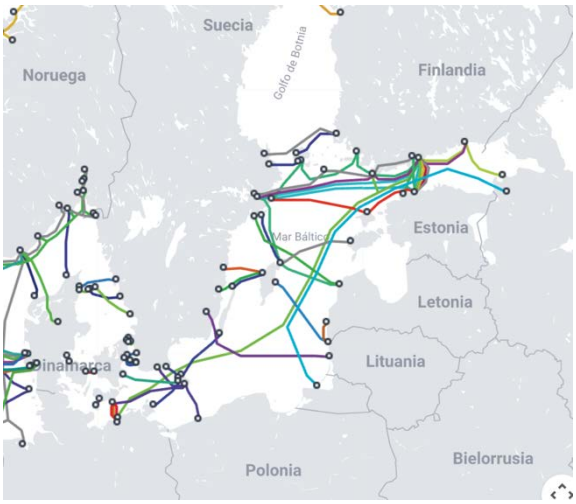

Illustration2 . Submarine cables in the Baltic Sea (Submarine Cable Map, 2025)

From a Eurasian perspective, Russia is portrayed in the literature as a revisionist power seeking to alter the European *status quo* through military pressure, grey-zone operations and the instrumental use of critical infrastructure[59].

The highly militarised Kaliningrad enclave plays a central role as a forward platform for projection and surveillance of the 'NATO lake'[60] [61].

Furthermore, investment in specialised units, such as the Main Directorate for Deep-Sea Research (GUGI), and in platforms capable of operating on subsea infrastructure

[55] KALEDIN, N. V. and ELATSKOV, A. V. *Op. cit.*
[56] O'RIORDAN. *Op. cit.*
[57] SWISTEK, G. and PAUL, M. *Op. cit.*
[58] POHORYLES, D. *Risks and protection of subsea cable networks* (EUR 40292 EN). Joint Research Centre, European Commission, 2025. Available at: https://doi.org/10.2760/701694
[59] CHARALAMBIDES, Y. *Op. cit.*
[60] KAUSHAL, S. 'Stalking the seabed: How Russia targets critical undersea infrastructure', *RUSI Commentary*. Royal United Services Institute, 2023. https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure
[61] KALEDIN, N. V. and ELATSKOV, A. V. *Op. cit.*

reinforces the perception that cables constitute a key element of Russia's national security strategy[62] [63] [64].

Illustration3 . Ownership of submarine cables and cable incidents (O'Riordan, 2025)

Although China is not a coastal state, its strategic presence in the Baltic Sea has increased indirectly. Within the framework of the Digital Silk Road, Beijing seeks to dominate key segments of the submarine cable supply chains — from their financing to their operation, through companies such as HNM Technologies[65] — as a tool for geopolitical influence, access to data and the reinforcement of structural dependencies, which has been described as a form of 'cable diplomacy'[66] [67].

[62] INSIKT GROUP. *Op. cit.*
[63] KAUSHAL. *Op. cit.*
[64] LOIK. *Op. cit.*
[65] ZHANG, J. 'Heading in the direction of bifurcated networks: Hong Kong's evolution amidst the global submarine cable system', *Asian Review of Political Economy*, 3(8). 2024. Available at: https://doi.org/10.1007/s44216-024-00029-1
[66] KUMAR, R. 'Securing the Digital Seabed: Countering China's Underwater Ambitions', *Journal of Indo-Pacific Affairs*, 46(4). 2023. Available at: https://media.defense.gov/2023/Nov/14/2003340185/-1/-1/1/FEATURE%20KUMAR%20-%20JIPA.PDF/FEATURE%20KUMAR%20-%20JIPA.PDF
[67] ROSS, N. and VENCILL, M. 'Digital Silk Road Peace: Subsea Cable Connections to the ICT', *Miltre.org*. 2024. Available at: https://www.mitre.org/news-insights/publication/digital-silk-road-peace-subsea-cable-connections-ict

In the Baltic, this presence is manifested primarily through merchant ships or container vessels involved in incidents that have affected critical infrastructure, such as the case of the New Polar Bear in 2023[68], or the subsequent suspicions surrounding the Yi Peng 3[69].

Although the attribution of intent remains uncertain, these episodes have reinforced the perception in the Baltic capitals that control of cables equates to control of data and, ultimately, to a growing capacity for geopolitical influence and pressure[70] [71].

Structural factors in the Baltic region

A fragmented legal framework

The legal environment of the Baltic Sea is characterised by legal fragmentation stemming from the United Nations Convention on the Law of the Sea (UNCLOS), which divides the maritime space into multiple zones with distinct legal regimes, creating gaps and ambiguities that hostile actors can exploit with little risk[72].

The protection of submarine cables thus takes place within a complex political framework, in which exclusive economic zones (EEZs), continental shelves, national and European competences, as well as the involvement of private operators, all overlap, making coordination in the event of incidents impossible[73].

The freedom of navigation provided for by UNCLOS allows ships flying flags of convenience or linked to the Russian *shadow fleet* to operate with a high degree of opacity in the Baltic EEZs[74] . Although coastal states hold rights over resources, their

[68] BERMINGHAM, F. 'Beijing admits Chinese ship destroyed key Baltic gas pipeline "by accident"', *South China Morning Post*. 12 August 2024. https://www.scmp.com/news/china/diplomacy/article/3274120/china-admits-hong-hong-flagged-ship-destroyed-key-baltic-gas-pipeline-accident
[69] MILNE, R., & TELLING, O. 'Chinese vessel spotted where Baltic Sea cables were severed', *Financial Times*. 19 November 2024. https://www.ft.com/content/383516a5-02db-46cf-8caa-a7b26a0a1bb2
[70] *REUTERS.* "Chinese ship linked to Baltic Sea cable breach resumes voyage", *Reuters*. 21 December 2024. https://www.reuters.com/world/chinese-ship-linked-baltic-sea-cable-breach-resumes-voyage-2024-12-21/
[71] PANCEVSKI, B. "Exclusive | Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables", *Wall Street Journal*. 27 November 2024. https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1
[72] UNITED NATIONS. *United Nations Convention on the Law of the Sea*. UN, 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
[73] BUEGER and LIEBETRAU. *Op. cit.*
[74] UNITED NATIONS. *Op. cit.*

capacity to enforce regulations on foreign vessels is limited, particularly under the regime of innocent passage, which facilitates the exploitation of regulatory loopholes[75].

This situation gives rise to two main problems.

Firstly, jurisdictional evasion, as a vessel can leave the EEZ before conclusive evidence of incidents exists. Consequently, the investigation is dependent on the often-insufficient cooperation of the flag state[76].

Secondly, there is a problem of evidence. Although damage can be detected quickly, proving intent requires lengthy investigations that facilitate plausible deniability and limit the capacity to respond[77].

Redundancy and bottlenecks

Although cable density in the Baltic has increased, many systems still lack sufficient redundancy—that is, alternative routes capable of taking over traffic if a link fails—which increases their vulnerability: in several sections, a single cable can cause significant disruptions if damaged[78] . Despite their protective layers, fibre-optic cables remain highly sensitive to external impacts (anchors, nets or underwater debris)[79] [80].

Added to this lack of redundancy is the existence of *choke points,* where the concentration of infrastructure prevents truly independent routes and increases the risk of multiple failures[81].

The clearest example is the Gulf of Finland, a narrow corridor congested by heavy maritime traffic[82] . This congestion was a key factor in the Eagle S incident in 2024, which

[75] MUUGA, E. *et al. Security threats to the undersea connections related critical infrastructure of the Baltic States: The Baltic Sea in the focus of hybrid warfare* (2nd ed.). Estonian Academy of Security Sciences. 2025. Available at: https://digiriiul.sisekaitse.ee/handle/123456789/2707
[76] Ibid.
[77] BUEGER and LIEBETRAU. *Op. cit.*
[78] MAULDIN, A., CONSTABLE, M. & BURDETTE, L. *The Future of Submarine Cable Maintenance*. 2025. https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/The%20Future%20of%20Submarine%20Cable%20Maintenance_%20Trends%2C%20Challenges%2C%20and%20Strategies.pdf
[79] EUROPEAN MARITIME SAFETY AGENCY (EMSA). *Annual Overview of Marine Casualties and Incidents. 2025*. https://www.emsa.europa.eu/accident-investigation-publications/annual-overview/download/8329/2713/23.html
[80] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *Subsea Cables - What is at stake?* 2023. https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf
[81] HIMKA, S. 'Baltic Sea Undersea Cable Security', *The Henry M. Jackson School of International Studies* (University of Washington). 2025. https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/
[82] Ibid.

illustrated how limited redundancy and spatial concentration can trigger systemic failures[83].

High density and concentration of digital infrastructure

The Baltic Sea is one of the most densely cabled maritime areas in the world[84] [85] . Figure 4 shows the dense network connecting Scandinavia, the Baltic States, Poland and Germany, with branches towards Russia and Kaliningrad.

These cables form the 'nervous system' of the global economy, as they carry almost all international internet and financial traffic; there are no viable satellite alternatives due to their lower capacity and higher cost[86] [87] .

The Baltic sections link strategic digital hubs in northern and central Europe, making the region a critical point in the European digital ecosystem, where a disruption in connectivity can have a knock-on effect across multiple countries and sectors[88].

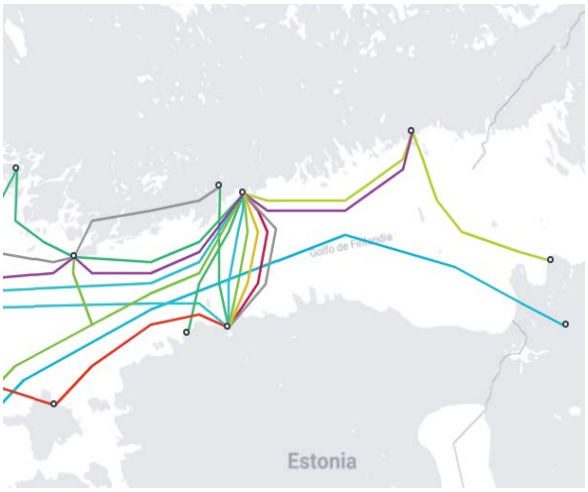

Illustration4 . Concentration of submarine cables in the Gulf of Finland (TeleGeography, 2025)

Shallow water depth and physical accessibility of the seabed

The shallow bathymetry of the Baltic Sea (see Figure 5) is by far one of the most critical physical factors in relation to the vulnerability of its submarine cables.

With an average depth of just 54 metres[89], access to the seabed is exceptionally easy, exposing the infrastructure to a considerable range of threats[90] . This accessibility creates

[83] LOTT. *Op. cit.*
[84] LOIK. *Op. cit.*
[85] POHORYLES. *Op. cit.*
[86] FRASCÀ, D. and GALANTINI, L. 'Towards a new European security architecture', *European Liberal Forum*. 2023. https://www.liberalforum.eu/publications/towards-a-new-european-security-architecture
[87] WASIUTA, O. *Russian threats to the submarine internet cable infrastructure*, Zeszyty Naukowe SGSP, 87, 2023, pp. 9–26. Available at: https://doi.org/10.5604/01.3001.0053.9127
[88] MAULDIN, A., CONSTABLE, M. and BURDETTE, L. *Op. cit.*
[89] POHORYLES. *Op. cit.*
[90] SEVILLANO PIRES, L., FARIZA, I. and TORRALBA, C. 'Submarine cables: The weakest link in Europe's strategic infrastructure', *El País Internacional*. 2025. https://english.elpais.com/international/2025-03-11/submarine-cables-the-weakest-link-in-europes-strategic-infrastructure.html?utm

an environment in which accidental damage or deliberate action can be carried out using non-specialised means[91].

An extreme example is provided by the C-Lion1 cable, which connects Finland with Germany and runs in certain sections through areas as shallow as 20 metres[92] . In such conditions, a conventional anchor—standard civilian equipment—ceases to be a harmless object and becomes a potential vector of attack.

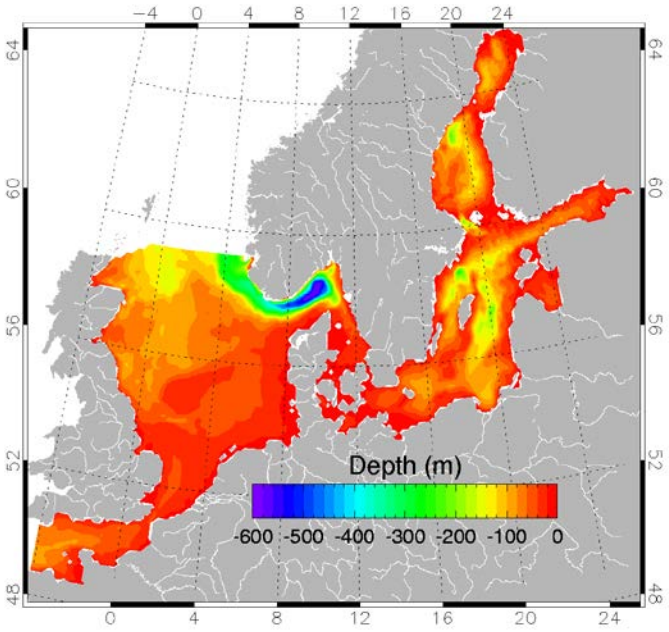

Figure 5. Depth map of the Baltic Sea (Woge, 2013)

The sabotage of submarine cables has become one of the most visible manifestations—if not the primary one—of the hybrid warfare strategy deployed by Russia within the territory of the European Union and NATO[93].

This problem is exacerbated by the inherent limitations of tracking movements in the maritime environment—at sea, any vessel can deactivate its tracking systems without leaving verifiable records—[94].

The lack of transparency is even greater in the underwater domain, where activities carried out on the seabed rarely yield conclusive evidence. Damage to infrastructure,

[91] POHORYLES. *Op. cit.*
[92] *20MINUTOS INTERNATIONAL. Op. cit.*
[93] LATSCHAN, T. 'Damaged cables in the Baltic: hybrid warfare at sea?', *Deutsche Welle*. 21 November 2024. https://www.dw.com/es/cables-da%C3%B1ados-en-el-b%C3%A1ltico-guerra-h%C3%ADbrida-en-el-fondo-del-mar/a-70853517
[94] CALDWELL. *Op. cit.*

when detected, usually comes to light too late to clearly identify those responsible, and even when material evidence—such as remains of anchors or trawl nets—is recovered, this rarely allows the incident to be attributed to a specific actor or the intentionality of the action to be demonstrated[95].

It is no coincidence that, according to the International Cable Protection Committee (ICPC), over 70% of damage to submarine cables is attributed to accidental human activities, which helps to reinforce a structurally ambiguous environment in which the boundary between accident and attack remains blurred.

Difficulty of repair and logistical constraints

The shallow depth of the Baltic seabed makes it easier for submarine cables to be damaged and, at the same time, complicates their repair. This combination of high exposure and limited capacity for immediate response constitutes a structural factor that undermines regional resilience[96]. When damage is easy to inflict and repairs are slow, the asymmetry between attack and recovery becomes critical.

The technical repair sequence is complex and depends on scarce resources. Firstly, a specialised cable-laying vessel must be mobilised, the availability of which is determined by its location, its workload and the small size of the European fleet[97]. This bottleneck causes initial delays even before the operation itself begins.

Once the vessel reaches the affected point, the entire process of precisely locating the cable, hoisting, splicing and re-laying takes between 5 and 15 days under favourable conditions[98] . In adverse weather conditions—which are frequent in the Baltic—these timescales can be significantly extended.

Taken together, the structural constraints of the Baltic Sea—a fragmented legal framework, shallow waters, a high concentration of infrastructure, limited redundancy, geographical bottlenecks and the logistical complexity of repairs—create a particularly vulnerable environment.

[95] MUUGA *et al*. *Op. cit.*
[96] MAULDIN, CONSTABLE and BURDETTE. *Op. cit.*
[97] Ibid.
[98] KOTTASOVÁ, I., STOCKWELL, B. and MURPHY, P. 'Two undersea cables in the Baltic Sea disrupted, sparking warnings of possible "hybrid warfare"', *CNN World*. 2024. https://www.cnn.com/2024/11/18/europe/undersea-cable-disrupted-germany-finland-intl

The accessibility of the seabed makes it easier to interfere with cables using non-specialised means, whilst the scarcity of alternative routes and available cable-laying vessels substantially prolongs any disruption.

This asymmetry between the ease of causing damage and the difficulty of repair makes Baltic submarine cables particularly attractive targets in contexts of strategic competition and hybrid warfare.

Challenges for NATO and European Union powers

Limitations of surveillance and control efforts in the Baltic maritime domain

The vastness of the maritime space poses structural challenges to surveillance and control in the Baltic Sea, limiting full and permanent monitoring[99] . Although the Automatic Identification System (AIS) allows for partial monitoring of traffic, its effectiveness is limited, as transponders can be easily switched off or tampered with[100].

These shortcomings are exacerbated underwater. Underwater surveillance requires acoustic sensors and specialised technologies that are costly and rarely deployed in the region[101], and most vessels are not equipped to use them[102] . Even emerging tools such as Distributed Acoustic Sensing (DAS) face obstacles: in an environment with heavy maritime traffic, background noise makes it difficult to distinguish anomalous signals from ordinary activity[103].

In this context, the *EU Maritime Security Strategy 2023* (EUMSS-23) acknowledges the existence of adequate capabilities for surface surveillance[104], but these remain insufficient for comprehensive protection of the underwater domain[105].

[99] CONTE DE LOS RÍOS. *Op. cit.*
[100] BERNABÉ *et al*. *Op. cit.*
[101] BUEGER and LIEBETRAU. *Op. cit.*
[102] MUUGA *et al*. *Op. cit.*
[103] BUEGER and LIEBETRAU. *Op. cit.*
[104] COUNCIL OF THE EUROPEAN UNION AND EUROPEAN COMMISSION. *European Union Maritime Security Strategy (EUMSS): Revised action plan.* 2023. https://oceans-and-fisheries.ec.europa.eu/document/download/57c32475-1dea-47d7-8bcb-92d8a2d0f056_en?filename=2018-06-26-eumss-revised-action-plan_en.pdf
[105] CONTE DE LOS RÍOS. *Op. cit.*

Digital sovereignty and geopolitical competition over the seabed

Various geopolitical analyses have pointed out that coastal states, whilst avoiding direct accusations against Russia or China, interpret the escalation of damage to cables and pipelines as part of a scenario of hybrid threats, in which both actors, along with others, feature as likely suspects[106].

Overlaying this perception is growing European concern about technological dependence on external suppliers in essential segments of the submarine cable network, in a context where strategic autonomy is at the heart of the European Union's security policy[107].

The presence of Chinese companies in the consortia responsible for the deployment, maintenance and operation of this infrastructure—including strategic segments in the Baltic—has raised fears about systemic vulnerabilities that are difficult to control[108].

In this context, the relationship between China and the Baltic states goes far beyond trade or the presence of ships on maritime routes. It forms part of a structural competition for control of the 'digital seabed', a sphere where technological interdependence is intertwined with strategic rivalry and where any incident—including those officially classified as maritime accidents—can act as an ambiguous episode that reinforces pre-existing tensions[109].

Ultimately, the combination of infrastructure density, the centrality of digital flows, the presence of actors with divergent interests, and fragmented governance creates an environment that fosters vulnerability and ambiguity.

Western responses and the limits of collective action

Western responses to the rise in incidents in the Baltic Sea reflect a gradual, though still incomplete, adaptation to hybrid threats. Within the alliance, NATO is strengthening the monitoring of submarine infrastructure and integrating cable protection into its maritime posture through joint exercises. In parallel, the European Union has placed this issue at

[106] O'RIORDAN. *Op. cit.*
[107] KARVONEN, J. 'Why Europe needs a Strategic Roadmap for Submarine Cable Resilience', *Laurea Journal*. 24 October 2025. https://journal.laurea.fi/why-europe-needs-a-strategic-roadmap-for-submarine-cable-resilience/#1bece0b2
[108] BUEGER, LIEBETRAU and FRANKEN. *Op. cit.*
[109] Ibid.

the centre of its regulatory agenda, recognising submarine cables as critical assets with a pan-European impact through instruments such as the *NIS2 Directive* and the *Cable Security Action Plan*[110] [111].

The practical implementation of these initiatives is limited by the fragmentation of responsibilities between public and private actors, as well as by gaps in information sharing and funding shortfalls to ensure continuous monitoring—problems widely highlighted in the specialist literature[112] [113].

In addition to these institutional constraints, there are operational factors specific to the maritime domain. Inspection of the seabed requires specialised vessels and sensors, the availability of which is limited, which delays the verification of damage and the collection of evidence[114].

This technical complexity is reflected in the legal and political spheres: although the EU's 2023 Maritime Security Strategy recognises the critical vulnerability of our submarine cables and the need to strengthen detection and attribution tools, the lack of an up-to-date international framework limits the state's ability to respond. Existing instruments, such as the 1884 Convention on the Protection of Submarine Cables and UNCLOS, do not adequately address emerging technological threats or the growing strategic importance of this infrastructure[115].

Added to this is the increased strategic pressure stemming from the militarisation of the Arctic, Russian manoeuvres in the Baltic and the greater Chinese presence in European ports[116].

Against this backdrop, some governments have called for more forceful responses. In 2024, a report by the British Parliament recommended going beyond the mere public

[110] FRASCÀ, D. and GALANTINI, L. *Op. cit.*
[111] POHORYLES. *Op. cit.*
[112] MUUGA *et al*. *Op. cit.*
[113] SWISTEK and PAUL. *Op. cit.*
[114] BUEGER and LIEBETRAU. *Op. cit.*
[115] *UNCLOSDEBATE*. 'Protection of undersea cables in Article 113 of UNCLOS is insufficient considering their critical importance'. https://www.unclosdebate.org/evidence/2135/protection-underseas-cables-article-113-unclos-insufficient-considering-their-critical ?
[116] BERMINGHAM. *Op. cit.*

attribution of acts of sabotage and exploring additional preventive and punitive measures[117].

However, the difficulty of attributing responsibility creates a legal vacuum. Authors such as Hartmann propose revisiting the use of Article 101 of UNCLOS on piracy, although they warn of its incompatibility with state attribution. Even so, the individual prosecution of those responsible could have some deterrent effect, albeit limited[118].

From a structural perspective, the European Union Agency for Cybersecurity emphasises that the resilience of cables requires a multi-level and multinational approach, as no single state can protect a transnational network on its own[119] . This reality has driven growing cooperation between the EU and NATO, with the former providing regulation, funding and relations with private operators, and the latter providing military capabilities, advanced surveillance and deterrence[120] [121].

EU–NATO cooperation has been institutionalised through the Joint Declarations of 2016, 2018 and 2023, and the creation in 2023 of the EU–NATO Task Force on critical infrastructure resilience, which has formulated recommendations on information sharing, vulnerability assessment and coordinated incident response, with a particular focus on submarine cables[122] [123].

At the operational and regulatory level, NATO has stepped up surveillance of the seabed, whilst the EU has developed instruments such as the Cable Security Action Plan (2025), the MARSUR network and the strengthening of the Common Information Sharing Environment (CISE). These instruments are aimed at improving situational awareness, as well as incident prevention and response[124] [125].

---

[117] JOINT COMMITTEE ON THE NATIONAL SECURITY STRATEGY. *Subsea telecommunications cables: resilience and crisis preparedness*. 2024. https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/723/report.html
[118] Ibid.
[119] ENISA. *Op. cit.*
[120] LOIK. *Op. cit.*
[121] BUEGER, LIEBETRAU and FRANKEN. *Op. cit.*
[122] NORTH ATLANTIC TREATY ORGANISATION. 'NATO and the EU set up taskforce on resilience and critical infrastructure', *NATO*. 2023. https://www.nato.int/en/news-and-events/articles/news/2023/01/11/nato-and-the-eu-set-up-taskforce-on-resilience-and-critical-infrastructure
[123] *EU-NATO Task Force on Resilience of Critical Infrastructure. Final Assessment Report.* 2023. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf
[124] CONTE DE LOS RÍOS. *Op. cit.*
[125] EUROPEAN COMMISSION. *EU Action Plan on Cable Security: Mapping and risk assessment approach agreed by group of Member States and providers*. 2025. https://digital-strategy.ec.europa.eu/en/news/eu-action-plan-cable-security-mapping-and-risk-assessment-approach-agreed-group-member-states-and

Studies on the Baltic Sea agree that the states in the region lack sufficient resources for autonomous protection; consequently, the solution lies in a combination of national capabilities and EU–NATO cooperation, based on shared surveillance, deterrence, regulation and funding[126].

In summary, although gaps and asymmetries remain, the protection of submarine cables has established itself as one of the most urgent and tangible pillars of EU–NATO cooperation in the face of hybrid threats, particularly in highly vulnerable regions such as the Baltic Sea[127].

Conclusions

The analysis carried out confirms the hypothesis put forward: the physical, legal and geopolitical factors of the Baltic Sea converge to make submarine cables a prime vector for hybrid warfare, against which the response capabilities of the European Union and NATO remain insufficient[128].

The shallow water depth, the density of critical infrastructure, the accessibility of the seabed and the difficulty of repair facilitate both accidental and hostile damage, whilst complicating early detection and the conclusive attribution of responsibility, blurring the line between the accidental and the deliberate[129].

Added to this is the structurally ambiguous nature of the maritime domain. The absence of witnesses, the vastness of the operational space, the possibility of disabling tracking systems, and the technical limitations of underwater investigations create a scenario conducive to covert operations[130] [131].

As the literature on hybrid warfare demonstrates, these actions deliberately operate below the threshold of armed conflict and exploit state vulnerabilities through plausible deniability tactics[132] [133] . In the Baltic, this ambiguity is intensified by heavy maritime

[126] MIĘTKIEWICZ, R. 'Hybrid threats in the Baltic Sea: The results of analysis of countermeasure options', *Terrorism – studies, analyses, prevention*, special edition. 2025, pp. 35–71. https://doi.org/10.4467/27204383TER.25.002.21505
[127] BUEGER, LIEBETRAU and FRANKEN. *Op. cit.*
[128] MAULDIN and BUDETTE. *Op. cit.*
[129] BURGER. *Op. cit.*
[130] BERNABÉ *et al*. *Op. cit.*
[131] MUUGA *et al*. *Op. cit.*
[132] OGRYZKO and RIZZI. *Op. cit.*
[133] RID and BUCHANAN. *Op. cit.*

traffic, which generates 'statistical noise' from seemingly accidental incidents, making it difficult to prove intent[134].

The legal dimension reinforces these conclusions. Although the law of the sea establishes a basic framework, its gaps are particularly evident in the protection of submarine cables.

Limited jurisdiction within the exclusive economic zone, the difficulty of investigating sabotage once a vessel has left coastal jurisdiction, and the obsolescence of regulatory frameworks such as the 1884 Convention highlight that European states lack sufficient tools to effectively prevent, attribute or sanction hybrid activities[135] . Consequently, Brussels, Washington and London have emphasised the need to modernise international frameworks and strengthen the regulatory architecture protecting these critical infrastructures[136].

On the geopolitical front, since 2022 the Baltic has established itself as an area particularly exposed to strategic tensions. Its quasi-status as a 'NATO lake', Russian militarisation in Kaliningrad and China's growing involvement in digital sovereignty are intensifying competition for control of the seabed[137].

The combination of plausible accidentalities, conflicting interests and strategic pressure confirms that the vulnerability of the cables is both technical and political[138] .

These findings show that the Baltic is a paradigmatic space for contemporary hybrid warfare dynamics.

As long as difficulties persist in attributing responsibility, physically protecting the seabed, coordinating multilateral responses and equipping existing frameworks with operational capacity, the EU and NATO will face a structural asymmetry against actors operating with low costs and high strategic impact[139].

Strengthening resilience, updating legal frameworks and deepening EU–NATO cooperation thus emerge as crucial priorities for European security in the coming decades[140].

[134] CAREY. *Op. cit.*
[135] HARTMANN. *Op. cit.*
[136] CONTE DE LOS RÍOS. *Op. cit.*
[137] CODREANU. *Op. cit.*
[138] MAULDIN, CONSTABLE, and BURDETTE. *Op. cit.*
[139] BRAW. *Op. cit.*
[140] COUNCIL OF THE EUROPEAN UNION AND EUROPEAN COMMISSION. *Op. cit.*

*Marta Molina Urosa, Javier Lafuente Capó, Manuel Lopera Rodríguez, Laura Ruiz Sancho, Gerard Terrés Pueyo, Pablo García Hernández**Hernández****

Lecturer and researcher at Comillas University (ICAI-ICADE-CIHS), parliamentary adviser to the Congress of Deputies, programme manager at Novaindef, communications analyst at the Operations Command, holder of a Master's degree in Diplomacy and International Relations, Lieutenant in the Spanish Navy