ieee.es
Instituto Español de Estudios Estratégicos

Documento de
Investigación

03/2026 6 de mayo de 2026

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

Infraestructura crítica en contexto de guerra híbrida: cables submarinos, competición geopolítica y vulnerabilidad estructural en el mar Báltico

Visitar la WEB

Recibir BOLETÍN ELECTRÓNICO

Infraestructura crítica en contexto de guerra híbrida: cables submarinos, competición geopolítica y vulnerabilidad estructural en el mar Báltico

Resumen:

Este artículo examina la creciente vulnerabilidad de los cables submarinos en el mar Báltico en el contexto de la competencia geopolítica. Las características físicas de estas infraestructuras, combinadas con un marco jurídico fragmentado, caracterizado por dificultades de atribución y ambigüedades normativas, generan condiciones propicias para operaciones de guerra híbrida en la denominada zona gris.

En un entorno regional cada vez más tensionado, los cables submarinos se han convertido en un vector estratégico para la realización de actividades disruptivas por debajo del umbral del conflicto armado.

El artículo desarrolla un marco conceptual para analizar la relevancia estratégica de estas infraestructuras y examina las dinámicas geopolíticas y los condicionantes estructurales que incrementan su vulnerabilidad en el mar Báltico.

Asimismo, evalúa las respuestas de la Unión Europea y la OTAN, e identifica los avances recientes y las limitaciones persistentes en su capacidad de disuasión, atribución y respuesta ante amenazas híbridas.

Palabras clave:

Cables submarinos, geopolítica, guerra híbrida, Rusia, China, infraestructura crítica.

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

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.

Cómo citar este documento:

MOLINA UROSA, Marta *et al. Infraestructura crítica en contexto de guerra híbrida: cables submarinos, competición geopolítica y vulnerabilidad estructural en el mar Báltico*. Documento de Investigación IEEE 03/2026. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

En un mundo profundamente interconectado, los cables submarinos constituyen la columna vertebral de la economía de las telecomunicaciones a escala global: más del 99 % del tráfico internacional de datos y cerca del 90 % de las comunicaciones entre Europa y Estados Unidos dependen de esta red física de aproximadamente 500 cables que se extiende por más de 1,7 millones de kilómetros[1] [2].

Estos sistemas sostienen las comunicaciones gubernamentales, las transacciones financieras, los servicios en la nube, las cadenas de suministro y el acceso a la información de miles de millones de personas[3].

Su estatus como infraestructura crítica se evidencia en la magnitud de su vulnerabilidad: cada año se registran entre 150 y 200 averías en el mundo. Más aún, en 2023 el International Cable Protection Committee (ICPC) documentó más de 200 reparaciones, lo que equivale a más de tres incidentes por semana[4].

Aunque una gran parte de estos daños se atribuyen a causas accidentales —principalmente arrastres de anclas, errores de navegación o actividades pesqueras[5]—, la frontera entre accidente y sabotaje se ha vuelto cada vez más difusa.

Esta ambigüedad responde, en parte, a la propia naturaleza del dominio marítimo. El derecho del mar, pese a ofrecer un marco de referencia básico, resulta insuficiente para garantizar la protección y atribución de responsabilidades respecto a infraestructuras que se sitúan, en muchos casos, fuera de la jurisdicción penal directa de los Estados ribereños[6].

La posibilidad de desconectar los sistemas de identificación automática (AIS) —sistemas que transmiten la posición e identidad de los buques para garantizar la seguridad y

[1] INTERNATIONAL TELECOMMUNICATION UNION. «Submarine Cable Resilience», *ITU*. 2024. Disponible en: https://www.itu.int/digital-resilience/submarine-cables/
Nota: Todos los hipervínculos se encuentran activos con fecha de 9 de abril de 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. Disponible en: 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. Disponible en: https://big-europe.eu/publications/2025-04-11-geopolitics-of-baltic-subsea-infrastructure

facilitar el seguimiento[7]—, el empleo de banderas de conveniencia o la ausencia de testigos convierten el entorno submarino en un espacio propicio para operaciones en la zona gris y para la consecuente negación plausible[8].

Así, tanto buques civiles como actores estatales pueden operar bajo un velo de opacidad que dificulta el esclarecimiento de incidentes y ofrece oportunidades para la ejecución de acciones híbridas difíciles de rastrear.

Desde 2022, esta vulnerabilidad estructural ha adquirido una dimensión geopolítica adicional. La guerra de Ucrania transformó el mar Báltico —tradicionalmente percibido como un mar estable e interdependiente— en un espacio de confrontación estratégica entre el bloque euroatlántico y las potencias revisionistas[9] [10].

La adhesión de Finlandia y Suecia a la OTAN consolidó el perímetro aliado en la cuenca, mientras que la costa rusa y el enclave de Kaliningrado mantienen su función como plataforma de proyección militar[11] [12].

En este contexto, el mar Báltico resulta fundamental para las telecomunicaciones, la interoperabilidad militar, la seguridad energética y la resiliencia económica europea.

Esta centralidad estratégica se explica, en gran medida, por la configuración de su lecho marino, que alberga una red especialmente densa de cables submarinos que conectan a Estados de la Unión Europea (UE) y de la Organización del Tratado del Atlántico Norte (OTAN) entre sí y con Rusia, particularmente con el enclave de Kaliningrado[13] [14].

[7] CALDWELL, J. «Security or safety: what is AIS really for?», *CIMSEC*. 19 mayo de 2025. Disponible en: https://cimsec.org/security-or-safety-what-is-ais-really-for/
[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. Disponible en: 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. Disponible en: https://doi.org/10.1080/09700161.2022.2076303
[10] LOIK. *Op. cit.*
[11] KALEDIN, N. V. y ELATSKOV, A. V. «Geopolitical regionalisation of the Baltic area: The essence and historical dynamics», *Baltic Region*, 16(1). 2024, pp. 141-158. Disponible en: https://doi.org/10.5922/2079-8555-2024-1-8
[12] SWISTEK, G. y 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. y ELATSKOV, A. V. *Op. cit.*
[14] SWISTEK, G. y PAUL, M. *Op. cit.*

Estas infraestructuras están gestionadas por un entramado complejo de propietarios y operadores europeos, chinos, rusos y estadounidenses, lo que refleja una profunda interdependencia y, al mismo tiempo, las tensiones estratégicas inherentes a la región[15].

Conviene recordar que la titularidad de estos cables es privada, lo que plantea importantes desafíos en materia de atribución de incidentes, de reparación y de resiliencia estratégica.

En este contexto, el presente artículo tiene como objetivo analizar cómo la convergencia de condicionantes físicos, jurídicos y geopolíticos del mar Báltico convierte los cables submarinos en un vector privilegiado de guerra híbrida, frente al cual las capacidades de respuesta de la Unión Europea y la OTAN siguen siendo insuficientes.

Se examinan así los límites estructurales que enfrentan ambas organizaciones para la protección, la atribución y la respuesta, y se evalúan, asimismo, la evolución estratégica de la región y las acciones en la denominada zona gris.

Para ello, el trabajo se estructura en cinco apartados: en primer lugar, se establece el marco conceptual sobre guerra híbrida, zona gris y negación plausible; en segundo lugar, se revisan los incidentes recientes y la evolución del entorno báltico desde 2022; en tercer lugar, se analizan los condicionantes que explican la vulnerabilidad de las infraestructuras submarinas; en cuarto lugar, se estudian los desafíos que estas dinámicas plantean para la UE y la OTAN, especialmente en materia de vigilancia, atribución y soberanía digital; y, finalmente, se abordan las respuestas occidentales y los límites de la acción colectiva, con el fin de valorar la adaptación institucional ante un entorno marcado por la ambigüedad estratégica y la competencia geopolítica creciente.

Marco conceptual: guerra híbrida, zona gris y negación plausible

Para comprender la base analítica de este trabajo, es necesario abordar el concepto de guerra híbrida, un concepto consolidado por Frank Hoffman (2007). Hoffman la caracteriza como «diferentes modos de guerra, que incluyen modos convencionales, tácticas y formaciones irregulares, así como actos terroristas, incluida la violencia indiscriminada y el desorden público»[16].

[15] O'RIORDAN. *Op. cit.*
[16] HOFFMAN, F. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, 2007. Disponible en: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

La OTAN define la guerra híbrida como «una combinación amplia, compleja y adaptativa de medios convencionales y no convencionales, así como de medidas militares, paramilitares y civiles, tanto abiertas como encubiertas, empleadas de manera integrada por Estados y actores no estatales para alcanzar sus objetivos»[17].

Con el tiempo, esta lógica se ha traducido en acciones encubiertas, ambiguas e inciertas, cuya naturaleza dificulta la atribución clara de responsabilidades.

En este contexto emerge la *grey zone* (zona gris), entendida como un espacio de confrontación caracterizado por «acciones coercitivas agresivas, pero deliberadamente calculadas, para que permanezcan por debajo del umbral que pudiera generar una respuesta militar abierta»[18].

La eficacia de estas acciones reside en la ambigüedad: ni el autor de los hechos ni sus intenciones pueden atribuirse con certeza. Esta falta de atribución erosiona la capacidad de respuesta de los Estados, al limitar el uso de herramientas jurídicas y dificultar la movilización de consensos internacionales[19].

La atribución —esto es, la identificación concluyente del responsable de una acción hostil— constituye, por tanto, un elemento central en este tipo de escenarios[20]. No se trata únicamente de una cuestión técnica, sino también política y estratégica: atribuir permite convencer a aliados, comunicar a la opinión pública la existencia de un adversario y dotar de legitimidad a eventuales medidas de represalia o disuasión.

En ausencia de una atribución clara, la ambigüedad estratégica se convierte en un arma en sí misma. Cuando la probabilidad de ser identificado es baja, los agresores obtienen beneficios elevados con un riesgo reducido de represalias[21].

A esta ambigüedad se suma un componente clave en los conflictos contemporáneos: la *plausible deniability* (negación plausible). Tal como señalan Rid y Buchanan (2015), este

[17] ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE. *Declaración final de la Cumbre de Varsovia* (párr. 72). OTAN/NATO, 9 de julio de 2016. Disponible en: 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. Disponible en: https://press.armywarcollege.edu/monographs/428
[19] Ibid.
[20] OGRYZKO, L. y RIZZI, A. «Shallow seas and "shadow fleets": Europe's undersea infrastructure is dangerously vulnerable», *European Council on Foreign Relations*. 8 de abril de 2025. Disponible en: https://ecfr.eu/article/shallow-seas-and-shadow-fleets-europes-undersea-infrastructure-is-dangerously-vulnerable/
[21] RID, T. y BUCHANAN, B. «Attributing Cyber Attacks», *Journal of Strategic Studies*, 38(1-2). 2015, pp. 4-37. Disponible en: https://doi.org/10.1080/01402390.2014.977382

concepto permite a actores estatales o no estatales negar su implicación en acciones hostiles.

La negación plausible adquiere especial relevancia en entornos donde la recopilación, trazabilidad y verificación de evidencias resultan particularmente complejas, como el ámbito marítimo y, de manera específica, el que atañe a las infraestructuras submarinas y a los cables de comunicaciones[22] [23].

Hasta el momento, la negación plausible ha constituido la principal ventaja estratégica de los actores que han llevado a cabo operaciones híbridas contra infraestructuras críticas de esta naturaleza[24] [25].

En este contexto adquiere relevancia el concepto de accidentalidad marítima, que engloba incidentes no intencionados como el arrastre involuntario de anclas, fallos de navegación, interferencias derivadas de la pesca de arrastre o daños ocasionados por condiciones meteorológicas adversas[26] [27] [28].

Si bien estos eventos forman parte de la normalidad operativa del entorno marítimo, en el contexto estratégico actual esta categoría ha sido instrumentalizada por actores estatales y no estatales para encubrir acciones hostiles contra infraestructuras críticas, como cables y tuberías submarinas, aprovechando la apariencia de daño fortuito[29].

La posibilidad de presentar un sabotaje como un accidente refuerza la negación plausible y complica la atribución, consolidando así la lógica de la zona gris.

[22] BUEGER, C. y LIEBETRAU, T. «Critical maritime infrastructure protection: What's the trouble?», *Marine Policy*, 155. 2023, 105772. Disponible en: https://doi.org/10.1016/j.marpol.2023.105772
[23] 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
[24] RID, T. y BUCHANAN, B. *Op. cit.*
[25] OGRYZKO, L. y RIZZI, A. *Op. cit.*
[26] CLAKE, M. *Submarine Cable Protection and the Environment*. An Update from the ICPC (Issue 6). International Cable Protection Committee, ICPC, 2023. Disponible en: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_November_2025.pdf
[27] International Telecommunications Union. *Op. cit.*
[28] BUEGER, C. «What is maritime security?», *Marine Policy*, 53. 2015, pp. 159-164. Disponible en: https://doi.org/10.1016/j.marpol.2014.12.005
[29] INSIKT GROUP. «Global threats to submarine cable infrastructure», *Recorded Future*. 2023. Disponible en: https://www.recordedfuture.com/resources/russian-undersea-capabilities

Además, estos incidentes permiten interferir indirectamente en la política interna de los Estados miembros de la UE y la OTAN mediante tácticas híbridas, como el empleo de buques con sistemas de identificación desconectados[30].

La ambigüedad estratégica, reforzada por narrativas que justifican o minimizan los daños, beneficia tanto al presunto perpetrador —al sostener la negación plausible— como, en algunas ocasiones, al Estado afectado, que puede optar por no impugnar públicamente la versión accidental para evitar la escalada y preservar el *statu quo*[31] [32].

En suma, la interacción entre la guerra híbrida, la zona gris, la negación plausible, las dificultades de atribución y la normalización de la accidentalidad marítima configuran un entorno estratégico particularmente propicio para la coerción encubierta en el dominio submarino, como ilustra el caso del mar Báltico.

Incidentes recientes y evolución estratégica del entorno báltico

La invasión rusa de Ucrania en 2022 y la adhesión de Finlandia y Suecia a la OTAN transformaron el mar Báltico de un espacio relativamente inestable en un frente de confrontación estratégica. Esta nueva configuración del Báltico como un «lago OTAN»[33] [34] [35], que se detallará más adelante, ha incrementado la relevancia geopolítica de los incidentes en la región.

Desde 2023, los daños registrados en cables submarinos —especialmente en torno al Balticconnector y en enlaces entre Finlandia, Estonia y Suecia— evidencian una fragilidad creciente. Aunque inicialmente se atribuyeron a accidentes, la repetición de

[30] CORKMAN, A. «La OTAN busca reforzar la seguridad en el mar Báltico tras los constantes sabotajes rusos a los cables submarinos», *Infobae*. 2025. https://www.infobae.com/america/mundo/2025/01/14/los-lideres-balticos-de-la-otan-buscan-reforzar-la-seguridad-tras-los-constantes-sabotajes-a-los-cables-submarinos/?utm_source=chatgpt.com
[31] REICHBORN-KJENNERUD, E. y 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
[32] OGRYZKO, L. y RIZZI, A. *Op. cit.*
[33] CHARALAMBIDES, Y. *Op. cit.*
[34] LOIK. *Op. cit.*
[35] KALEDIN, N. V. y ELATSKOV, A. V. *Op. cit.*

patrones y su concentración espacial han incrementado las sospechas de intencionalidad encubierta[36] [37] [38].

Esta evolución se refleja también en los datos disponibles. Aunque en gran parte son reservados, las mencionadas 200 incidencias anuales resultan relevantes[39]. Desde 2023 se aprecia así un paso del fallo aislado al daño potencialmente coordinado, como muestran los incidentes más relevantes que se detallan a continuación.

- Octubre de 2023: el portacontenedores NewNew Polar Bear (bandera china) dañó dos cables y el Balticconnector por arrastre de ancla. Finlandia y Suecia calificaron el suceso como un accidente, derivado de un error operacional o negligencia asociada al deficiente estado del buque, aunque persistieron sospechas de intencionalidad que no pudieron probarse[40].
- Diciembre de 2024: el petrolero *Eagle S* (pabellón de las Islas Cook), vinculado a la *shadow fleet* rusa, cortó cinco cables y la interconexión Estlink 2. El surco de ancla de 90 km apuntaba a un patrón compatible con una negligencia grave; sin embargo, la localización del incidente en la zona económica exclusiva (ZEE) limitó la actuación de la jurisdicción finlandesa[41] [42]. El caso, actualmente recurrido por la fiscalía finlandesa, se ha interpretado como un episodio paradigmático de guerra híbrida[43].
- Enero de 2025: Suecia incautó el buque Vezhen (bandera maltesa y tripulación mayoritariamente búlgara) tras dañar un cable entre Letonia y Gotland. Aunque el

[36] BRAW, E. «How the Baltic Sea nations have tackled suspicious cable cuts», *Atlantic Council*. 26 de noviembre de 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/
[37] CODREANU, M. C. «Crossing the line: Severing undersea internet cables in geopolitical hotspots», *Policy Brief* n.º 76. New Strategy Center, 2025. https://www.newstrategycenter.ro/wp-content/uploads/2025/06/Codreanu_PB76_EN-1.pdf
[38] *THE ECONOMIST*. «Who is sabotaging underwater infrastructure in the Baltic Sea?». 22 de octubre de 2023. https://www.economist.com/europe/2023/10/22/who-is-sabotaging-underwater-infrastructure-in-the-baltic-sea
[39] INTERNATIONAL TELECOMMUNICATION UNION*. Op. cit.*
[40] BESCH, S. y BROWN, E. «Securing Europe's Subsea Data Cables», *Carnegie Endowment for International Peace*.16 de diciembre de 2024. Disponible en: https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables
[41] 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. Disponible en: https://doi.org/10.1080/00908320.2023.2265301
[42] BRAYANT, M. y *correspondent,* M. B. N. «Finland charges tanker crew members with sabotage of undersea cables», *The Guardian*. 11 de agosto de 2025. https://www.theguardian.com/world/2025/aug/11/finland-accuses-tanker-crew-sabotage-undersea-cables-anchor
[43] SWISSINFO. «Finlandia acusa a tres marineros de un petrolero por sabotear cables en el mar Báltico», *SWI swissinfo.ch*. 11 de agosto de 2025. https://www.swissinfo.ch/spa/finlandia-acusa-a-tres-marineros-de-un-petrolero-por-sabotear-cables-en-el-mar-báltico/89816031

incidente fue finalmente atribuido a un error humano, contribuyó a reforzar la percepción de riesgo en la región[44].

El caso de Estlink 2 resulta especialmente significativo. Su reparación se prolongó durante siete meses, en pleno invierno báltico, y las investigaciones revelaron la presencia de equipos de contraespionaje, así como un rastro de ancla coincidente con la trayectoria del Eagle S, lo que reforzó la tesis del sabotaje[45] [46]. Este episodio impulsó una intensificación de la cooperación en materia de vigilancia entre la OTAN y los países bálticos[47].

Aunque la mayoría de los incidentes documentados afectan a los cables submarinos, otras infraestructuras estratégicas también han sido objeto de ataques. En particular, los gasoductos Nord Stream 1 y Nord Stream 2 fueron saboteados en septiembre de 2022.

Las sospechas iniciales apuntaron a Rusia, si bien el Kremlin lo negó y alegó el elevado valor económico de los gasoductos para sus propios intereses[48]. La posterior detención en Alemania de un ciudadano ucraniano añadió complejidad al caso y evidenció que la confrontación híbrida en el mar Báltico se caracteriza por la ambigüedad, la atribución incierta y la pluralidad de actores[49], lo que supone un desafío para la disuasión y la respuesta colectiva.

[44] AHLANDER, J. y RINGSTROM, A. «Swedish authorities board ship seized over Baltic Sea cable breach», *Reuters*. 27 de enero de 2025. https://www.reuters.com/world/europe/swedish-authorities-board-ship-seized-over-baltic-sea-cable-breach-2025-01-27/

[45] 20MINUTOS INTERNACIONAL. «¿Córtó un barco chino los cables del Báltico? Investigan la ruta del carguero Yi Peng 3 y si fue el causante del sabotaje». 22 de noviembre de 2024. https://www.20minutos.es/noticia/5656513/0/suecia-dinamarca-investigan-buque-chino-causo-doble-sabotaje-baltico/

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

[47] Ibid.

[48] 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

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

Fecha	Infraestructura afectada	Actor o embarcación implicada	Tipo de daño	Conclusiones oficiales / estado de la investigación
Sept. 2022	**Gasoductos Nord Stream 1 y 2**	No identificado (sospechas diversas)	Explosiones submarinas	Autores no confirmados; sospechas iniciales hacia Rusia, posteriormente hacia posibles actores ucranianos; investigación aún abierta
Oct. 2023	**Balticconnector + 2 cables de telecomunicaciones**	NewNew Polar Bear (bandera china)	Arrastre de ancla	Considerado accidente por Suecia y Finlandia; sin pruebas de intencionalidad, aunque con fuerte sospecha estratégica
Dic. 2024	**Estlink 2 + 5 cables de telecomunicaciones**	Eagle S (Islas Cook, vinculado a *shadow fleet*)	Seccionamiento múltiple por arrastre de ancla	Evidencias de recorrido de 90 km; Finlandia interpreta sabotaje; limitaciones de jurisdicción; caso bajo recurso
Ene. 2025	**Cable Letonia–Gotland**	Vezhen (bandera maltesa)	Daño por arrastre o maniobra inapropiada	Investigado como posible sabotaje; finalmente clasificado como accidente por error humano
2024–2025	**Estlink 2 (reparación)**	—	Daños estructurales complejos	Reparación finalizada en agosto 2025; duración ~7 meses por complejidad técnica y meteorológica

Tabla 1. Incidentes en el mar Báltico (2022-2025). Elaboración propia

Condicionantes geopolíticos del mar Báltico

La región báltica puede entenderse como un sistema geopolítico articulado en torno al mar Báltico y los estrechos daneses, que integra espacios marítimos, costeros y terrestres, así como las principales rutas de comunicación entre puertos y territorios interiores (*hinterlands)*[50].

Ilustración 1. La región del mar Báltico (Savitz & Winston, 2024)

Se trata de un entorno caracterizado por la superposición de múltiples dominios —marino, geográfico, económico y estratégico— y por un elevado número de actores, que incluyen a países nórdicos, Estados bálticos y países de Europa Central, tanto miembros como no miembros de la OTAN. Esta diversidad configura una región en la que coexisten relaciones de cooperación y conflicto en distintas escalas y ámbitos[51] [52].

Desde el punto de vista geopolítico, el mar Báltico se ha consolidado como un enclave de carácter bipolar, situado en la interfaz entre el subsistema euroatlántico y el euroasiático.

Esta dinámica se traduce en una creciente confrontación entre un bloque báltico-euroatlántico —integrado por los Estados miembros de la UE y la OTAN— y un bloque báltico-eurasiático, centrado en Rusia y China[53].

Dentro de este marco más amplio, la región marítima báltica se configura como un foco de interés y conflicto geopolítico debido a la combinación de tres factores: (i) su condición casi consolidada de «lago OTAN»; (ii) la presencia militarizada de Rusia en Kaliningrado; y (iii) la existencia de una densa red de infraestructuras críticas —en particular cables

[50] KALEDIN, N. V. y ELATSKOV, A. V. *Op. cit.*
[51] Ibid.
[52] SWISTEK, G. y PAUL, M. *Op. cit.*
[53] CHARALAMBIDES, Y. *Op. cit.*

submarinos de telecomunicaciones— que enlazan entre sí a los Estados de la UE y de la Alianza, y que los conectan también con Rusia[54] [55] [56].

Desde la perspectiva euroatlántica, la adhesión de Finlandia (2023) y de Suecia (2024) a la OTAN ha reforzado de forma decisiva la percepción del Báltico como un «lago OTAN»[57] [58] [59], al situar prácticamente todo su litoral bajo el paraguas aliado. Para la Unión Europea, esta región resulta, además, estratégica para la cohesión del mercado único digital, dado que los cables submarinos garantizan la conectividad entre los Estados miembros y los países bálticos, así como la seguridad de las rutas comerciales y energéticas[60].

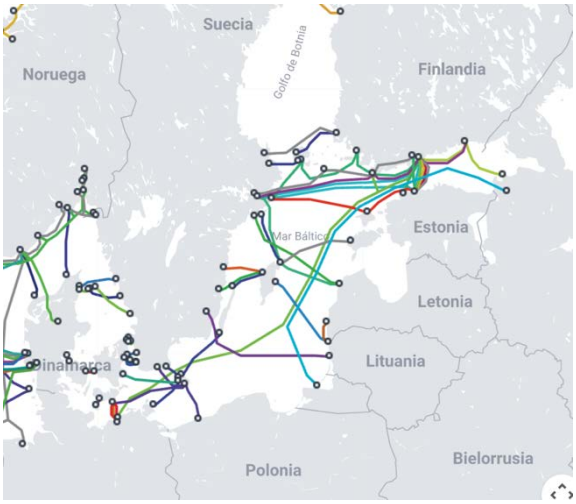

Ilustración 2. Cables submarinos en el mar Báltico (Submarine Cable Map, 2025)

Desde la perspectiva euroasiática, Rusia aparece en la literatura como una potencia revisionista que busca alterar el *statu quo* europeo mediante la presión militar, las operaciones en la zona gris y el uso instrumental de las infraestructuras críticas[61].

[54] 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. Disponible en: https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2022)702557
[55] LOIK. *Op. cit.*
[56] O'RIORDAN. *Op. cit.*
[57] KALEDIN, N. V. y ELATSKOV, A. V. *Op. cit.*
[58] O'RIORDAN. *Op. cit.*
[59] SWISTEK, G. y PAUL, M. *Op. cit.*
[60] POHORYLES, D. *Risks and protection of subsea cable networks* (EUR 40292 EN). Joint Research Centre, European Commission, 2025. Disponible en: https://doi.org/10.2760/701694
[61] CHARALAMBIDES, Y. *Op. cit.*

El enclave de Kaliningrado, altamente militarizado, desempeña un papel central como plataforma avanzada de proyección y vigilancia del «lago OTAN»[62] [63].

Asimismo, la inversión en unidades especializadas, como la Dirección Principal de Investigación de Aguas Profundas (GUGI), y en plataformas capaces de operar sobre infraestructuras submarinas refuerzan la percepción de que los cables constituyen un elemento clave de la estrategia de seguridad nacional rusa[64] [65] [66].

Ilustración 3. Propiedad de los cables submarinos e incidentes en cables (O'Riordan, 2025)

Aunque China no es un actor ribereño, su presencia estratégica en el mar Báltico se ha incrementado de forma indirecta. En el marco de la Digital Silk Road, Pekín busca dominar segmentos clave de las cadenas de suministro de cables submarinos —desde su financiación hasta su operación, a través de empresas como HNM Technologies[67]— como herramienta de influencia geopolítica, de acceso a datos y de refuerzo de

[62] 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
[63] KALEDIN, N. V. y ELATSKOV, A. V. *Op. cit.*
[64] INSIKT GROUP. *Op. cit.*
[65] KAUSHAL. *Op. cit.*
[66] LOIK. *Op. cit.*
[67] 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. Disponible en: https://doi.org/10.1007/s44216-024-00029-1

dependencias estructurales, lo que se ha descrito como una forma de «diplomacia del cable»[68] [69].

En el Báltico, esta presencia se manifiesta principalmente a través de buques mercantes o portacontenedores implicados en incidentes que han afectado a infraestructuras críticas, como el caso del NewNew Polar Bear en 2023[70], o las sospechas posteriores en torno al Yi Peng 3[71].

Aunque la atribución de intencionalidad sigue siendo incierta, estos episodios han reforzado en las capitales bálticas la percepción de que el control de cables equivale al control de los datos y, en última instancia, a una creciente capacidad de influencia y presión geopolítica[72] [73].

Condicionantes estructurales del entorno báltico

Un marco jurídico fragmentado

El entorno jurídico del mar Báltico está marcado por una fragmentación jurídica derivada de la Convención de las Naciones Unidas sobre el Derecho del Mar (UNCLOS), que divide el espacio marítimo en múltiples zonas con regímenes jurídicos distintos, lo que genera vacíos y ambigüedades que los actores hostiles pueden explotar con bajo riesgo[74].

La protección de los cables submarinos se inserta así en un marco político complejo, en el que se superponen zonas económicas exclusivas (ZEEs), plataformas continentales,

[68] KUMAR, R. «Securing the Digital Seabed: Countering China's Underwater Ambitions», *Journal of Indo-Pacific Affairs,* 46(4). 2023. Disponible en: https://media.defense.gov/2023/Nov/14/2003340185/-1/-1/1/FEATURE%20KUMAR%20-%20JIPA.PDF/FEATURE%20KUMAR%20-%20JIPA.PDF

[69] ROSS, N. y VENCILL, M. «Digital Silk Road Peace: Subsea Cable Connections to the ICT», *Miltre.org*. 2024. Disponible en: https://www.mitre.org/news-insights/publication/digital-silk-road-peace-subsea-cable-connections-ict

[70] BERMINGHAM, F. «Beijing admits Chinese ship destroyed key Baltic gas pipeline 'by accident'», *South China Morning Post*. 12 de agosto de 2024. https://www.scmp.com/news/china/diplomacy/article/3274120/china-admits-hong-hong-flagged-ship-destroyed-key-baltic-gas-pipeline-accident

[71] MILNE, R., & TELLING, O. «Chinese vessel spotted where Baltic Sea cables were severed», *Financial Times*. 19 de noviembre de 2024. https://www.ft.com/content/383516a5-02db-46cf-8caa-a7b26a0a1bb2

[72] *REUTERS.* «Chinese ship linked to Baltic Sea cable breach resumes voyage», *Reuters*. 21 de diciembre de 2024. https://www.reuters.com/world/chinese-ship-linked-baltic-sea-cable-breach-resumes-voyage-2024-12-21/

[73] PANCEVSKI, B. «Exclusive | Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables», *Wall Street Journal*. 27 de noviembre de 2024. https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1

[74] ORGANIZACIÓN DE LAS NACIONES UNIDAS. *United Nations Convention on the Law of the Sea*. ONU, 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

competencias nacionales y europeas, así como la participación de operadores privados, lo que imposibilita la coordinación ante incidentes[75].

La libertad de navegación prevista por la UNCLOS permite que buques con banderas de conveniencia o vinculados a la *shadow fleet* rusa operen con elevada opacidad en las ZEE bálticas[76]. Aunque los Estados ribereños poseen derechos sobre los recursos, su capacidad coercitiva sobre buques extranjeros es limitada, especialmente bajo el régimen de paso inocente, lo que facilita la explotación de lagunas normativas[77].

Esta situación genera dos problemas principales.

En primer lugar, la evasión jurisdiccional, al poder un buque abandonar la ZEE antes de que existan pruebas concluyentes de incidentes. De esta forma, la investigación queda supeditada a la cooperación, a menudo insuficiente, del Estado de bandera[78].

En segundo lugar, existe dificultad probatoria. Aunque la detección de daños es rápida, demostrar la intencionalidad requiere investigaciones prolongadas que favorecen la negación plausible y limitan la capacidad de respuesta[79].

Redundancia y cuellos de botella

Aunque la densidad de cables en el Báltico ha aumentado, muchos sistemas carecen aún de redundancia suficiente —esto es, de rutas alternativas capaces de asumir el tráfico si un enlace falla—, lo que incrementa su vulnerabilidad: en varios tramos, un único cable puede provocar interrupciones significativas si resulta dañado[80]. Pese a sus capas protectoras, los cables de fibra óptica siguen siendo muy sensibles a impactos externos (anclas, redes o restos submarinos)[81] [82].

---

[75] BUEGER y LIEBETRAU. *Op. cit.*
[76] ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Op. cit.*
[77] 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* (2.ª ed.). Estonian Academy of Security Sciences. 2025. Disponible en: https://digiriiul.sisekaitse.ee/handle/123456789/2707
[78] Ibid.
[79] BUEGER y LIEBETRAU. *Op. cit.*
[80] 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
[81] 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
[82] 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

A esta carencia de redundancia se suma la existencia de *choke points,* en los que la concentración de infraestructuras impide rutas verdaderamente independientes y aumenta el riesgo de fallos múltiples[83].

El caso más claro es el golfo de Finlandia, un corredor estrecho y saturado por un intenso tráfico marítimo[84]. Esta congestión fue determinante en el episodio del Eagle S en 2024, que ilustró cómo la limitada redundancia y la concentración espacial pueden desencadenar fallos sistémicos[85].

Alta densidad y concentración de infraestructura digital

El mar Báltico es uno de los espacios marítimos más densamente cableados del mundo[86] [87]. La ilustración 4 muestra la densa malla que conecta Escandinavia, los Estados bálticos, Polonia y Alemania, con ramales hacia Rusia y Kaliningrado.

Estos cables constituyen el «sistema nervioso» de la economía global, ya que transportan casi todo el tráfico internacional de Internet y financiero, sin que existan alternativas viables vía satélite, debido a su menor capacidad y su mayor coste[88] [89].

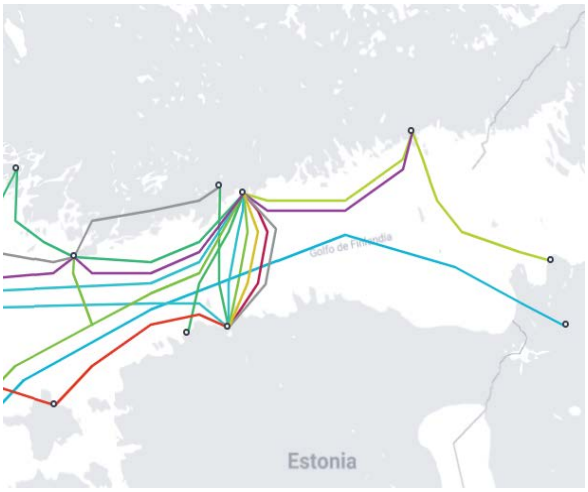

Ilustración 4. Concentración de cables submarinos en el golfo de Finlandia (TeleGeography, 2025)

Los tramos bálticos enlazan nodos digitales estratégicos de Europa septentrional y central, lo que convierte la región en un punto crítico del ecosistema digital europeo, en el que una interrupción en la conectividad puede generar efectos en cascada en múltiples países y sectores[90].

[83] HIMKA, S. «Baltic Sea Undersea Cable Security», *The Henry M. Jackson School of International Studies* (Universidad de Washington). 2025. https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/
[84] Ibid.
[85] LOTT. *Op. cit.*
[86] LOIK. *Op. cit.*
[87] POHORYLES. *Op. cit.*
[88] FRASCÀ, D. y GALANTINI, L. «Towards a new European security architecture», *European Liberal Forum*. 2023. https://www.liberalforum.eu/publications/towards-a-new-european-security-architecture
[89] WASIUTA, O. *Russian threats to the submarine internet cable infrastructure*, Zeszyty Naukowe SGSP, 87, 2023, pp. 9-26. Disponible en: https://doi.org/10.5604/01.3001.0053.9127
[90] MAULDIN, A., CONSTABLE, M. y BURDETTE, L. *Op. cit.*

Baja batimetría y accesibilidad física del lecho marino

La baja batimetría del mar Báltico (ver la ilustración 5) constituye, con diferencia, uno de los factores físicos más críticos en relación con la vulnerabilidad de sus cables submarinos.

Con una profundidad media de apenas 54 metros[91], el acceso al lecho marino es excepcionalmente sencillo, lo que expone la infraestructura a un abanico considerable de amenazas[92]. Esta accesibilidad crea un entorno en el que un daño accidental o una acción deliberada pueden ejecutarse con medios no especializados[93].

Un ejemplo extremo lo ofrece el cable C-Lion1, que conecta Finlandia con Alemania y cuyo tendido discurre en ciertos tramos por zonas de tan solo 20 metros de profundidad[94]. En tales condiciones, un ancla convencional —un equipo civil estándar— deja de ser un objeto inocuo y se convierte en un potencial vector de ataque.

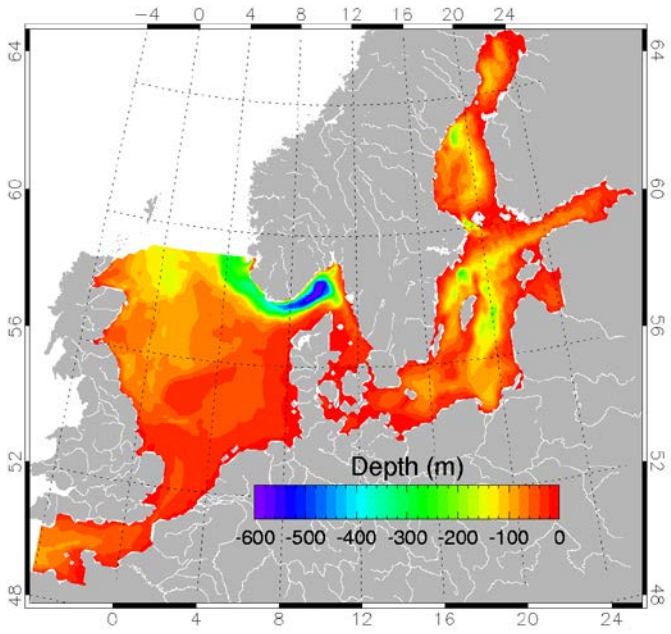

Ilustración 5. Mapa de profundidad en el mar Báltico (Woge, 2013)

[91] POHORYLES. *Op. cit.*
[92] SEVILLANO PIRES, L., FARIZA, I. y 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
[93] POHORYLES. *Op. cit.*
[94] *20MINUTOS INTERNATIONAL. Op. cit.*

El sabotaje de cables submarinos se ha convertido en una de las manifestaciones más visibles —si no la principal— de la estrategia de guerra híbrida desplegada por Rusia en territorio de la Unión Europea y de la OTAN[95].

Esta problemática se ve agravada por las limitaciones inherentes a la trazabilidad de movimientos en el entorno marítimo —en el mar, cualquier embarcación puede desactivar sus sistemas de rastreo sin dejar registros verificables—[96].

La opacidad se intensifica en el dominio submarino, en el que las actividades realizadas en el lecho marino rara vez generan pruebas concluyentes. Los daños en la infraestructura, cuando se detectan, suelen aparecer demasiado tarde para identificar con claridad a los responsables y, aun cuando se recuperan indicios materiales —como restos de anclas o redes de arrastre—, estos rara vez permiten atribuir el hecho a un actor concreto o demostrar la intencionalidad de la acción[97].

No es casual que, según el International Cable Protection Committee (ICPC), más del 70 % de los daños en cables submarinos se atribuyan a actividades humanas accidentales, lo que contribuye a reforzar un entorno estructuralmente ambiguo en el que la frontera entre accidente y ataque permanece difusa.

Dificultad de reparación y limitaciones logísticas

La escasa profundidad del lecho marino báltico facilita el daño a los cables submarinos y, al mismo tiempo, complica su reparación. Esta combinación de alta exposición y limitada capacidad de respuesta inmediata constituye un factor estructural que debilita la resiliencia regional[98]. Cuando dañar resulta sencillo y reparar, lento, la asimetría entre ataque y recuperación se vuelve crítica.

La secuencia técnica de reparación es compleja y depende de recursos escasos. En primer lugar, es necesaria la movilización de un buque cablero especializado, cuya disponibilidad está condicionada por su ubicación, su carga de trabajo y el reducido

[95] LATSCHAN, T. «Cables dañados en el Báltico: ¿guerra híbrida en el mar?», *Deutsche Welle*. 21 de noviembre de 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
[96] CALDWELL. *Op. cit.*
[97] MUUGA *et al*. *Op. cit.*
[98] MAULDIN, CONSTABLE y BURDETTE. *Op. cit.*

tamaño de la flota europea[99]. Este cuello de botella genera demoras iniciales incluso antes de que comience la operación propiamente dicha.

Una vez que el buque llega al punto afectado, el proceso completo de localización precisa del cable, izado, empalme y reinstalación requiere entre 5 y 15 días en condiciones favorables[100]. En situaciones meteorológicas adversas —frecuentes en el Báltico— estos plazos pueden ampliarse significativamente.

En conjunto, los condicionantes estructurales del mar Báltico —marco jurídico fragmentado, baja batimetría, elevada concentración de infraestructuras, limitada redundancia, cuellos de botella geográficos y complejidad logística de las reparaciones— configuran un entorno especialmente vulnerable.

La accesibilidad del lecho marino facilita la posibilidad de interferir con los cables mediante medios no especializados, mientras que la escasez de rutas alternativas y de buques cableros disponibles prolonga de forma sustancial cualquier disrupción.

Esta asimetría entre la facilidad del daño y la dificultad de la reparación convierte los cables submarinos bálticos en objetivos particularmente atractivos en contextos de competencia estratégica y guerra híbrida.

Desafíos para las potencias de la OTAN y la Unión Europea

Limitaciones del esfuerzo de vigilancia y control en el dominio báltico marítimo

La inmensidad del espacio marítimo plantea desafíos estructurales a la vigilancia y al control en el mar Báltico, lo que limita una supervisión plena y permanente[101]. Aunque el Automatic Identification System (AIS) permite monitorizar parcialmente el tráfico, su eficacia es limitada, ya que los transpondedores pueden apagarse o manipularse con facilidad[102].

Estas carencias se acentúan bajo el agua. La vigilancia submarina exige sensores acústicos y tecnologías especializadas, costosas y poco desplegadas en la región[103], y

[99] Ibid.
[100] KOTTASOVÁ, I., STOCKWELL, B. y MURPHY, P. «Two undersea cables in 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
[101] CONTE DE LOS RÍOS. *Op. cit.*
[102] BERNABÉ *et al*. *Op. cit.*
[103] BUEGER y LIEBETRAU. *Op. cit.*

la mayoría de las embarcaciones no están equipadas para utilizarlas[104]. Incluso herramientas emergentes como la Detección Acústica Distribuida (DAS) afrontan obstáculos: en un entorno con intenso tráfico marítimo, el ruido de fondo dificulta distinguir señales anómalas de la actividad ordinaria[105].

En este contexto, la *Estrategia de Seguridad Marítima de la UE de 2023* (EUMSS-23) reconoce la existencia de capacidades adecuadas para la vigilancia en superficie[106], pero estas siguen siendo insuficientes para una protección integral del dominio submarino[107].

Soberanía digital y competencia geopolítica por el fondo marino

Diversos análisis geopolíticos han señalado que los Estados ribereños, aun evitando acusaciones directas contra Rusia o China, interpretan la escalada de daños a cables y tuberías como parte de un escenario de amenazas híbridas, en el que ambos actores, junto con otros, figuran como sospechosos probables[108].

A esta percepción se superpone la creciente inquietud europea por la dependencia tecnológica de proveedores externos en segmentos esenciales de la red de cables submarinos en un contexto en el que la autonomía estratégica está en el centro de la política de seguridad de la Unión Europea[109].

La presencia de empresas chinas en los consorcios encargados del despliegue, mantenimiento y operación de estas infraestructuras —incluidos segmentos estratégicos en el Báltico— ha suscitado temores acerca de vulnerabilidades sistémicas difíciles de controlar[110].

En este contexto, la relación entre China y los Estados bálticos va mucho más allá del intercambio comercial o de la presencia de buques en rutas marítimas. Se inscribe en una competencia estructural por el control del «fondo marino digital», un ámbito donde la interdependencia tecnológica se mezcla con la rivalidad estratégica y donde cualquier

[104] MUUGA *et al*. *Op. cit.*
[105] BUEGER y LIEBETRAU. *Op. cit.*
[106] CONSEJO DE LA UNIÓN EUROPEA Y COMISIÓN EUROPEA. *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
[107] CONTE DE LOS RÍOS. *Op. cit.*
[108] O'RIORDAN. *Op. cit.*
[109] KARVONEN, J. «Why Europe needs a Strategic Roadmap for Submarine Cable Resilience», *Laurea Journal*. 24 de octubre de 2025. https://journal.laurea.fi/why-europe-needs-a-strategic-roadmap-for-submarine-cable-resilience/#1bece0b2
[110] BUEGER, LIEBETRAU y FRANKEN. *Op. cit.*

incidente —incluso los catalogados oficialmente como accidentes marítimos— puede actuar como un episodio ambiguo que refuerza tensiones preexistentes[111].

En definitiva, la combinación de densidad infraestructural, centralidad de los flujos digitales, presencia de actores con intereses divergentes y una gobernanza fragmentada configura un entorno que favorece la vulnerabilidad y la ambigüedad.

Respuestas occidentales y límites de la acción colectiva

Las respuestas occidentales al aumento de incidentes en el mar Báltico reflejan una adaptación gradual, aunque aún incompleta, a las amenazas híbridas. En el ámbito aliado, la OTAN está reforzando el seguimiento de infraestructuras submarinas e integrando la protección de cables en su postura marítima mediante ejercicios conjuntos. Paralelamente, la Unión Europea ha situado esta cuestión en el centro de su agenda regulatoria, reconociendo a los cables submarinos como activos críticos con impacto paneuropeo a través de instrumentos como la *Directiva NIS2* y el *Plan de Acción sobre seguridad de cables*[112] [113].

La aplicación práctica de estas iniciativas se ve limitada por la fragmentación de competencias entre actores públicos y privados, así como por las lagunas en el intercambio de información y los déficits de financiación para garantizar una monitorización permanente, problemas ampliamente señalados en la literatura especializada[114] [115].

A estas limitaciones institucionales se suman condicionantes operativos propios del dominio marítimo. La inspección del fondo marino requiere buques y sensores especializados cuya disponibilidad es reducida, lo que retrasa la verificación de daños y la recopilación de evidencias[116].

Esta complejidad técnica tiene su reflejo en el plano jurídico y político: aunque la *Estrategia de Seguridad Marítima de la UE* de 2023 reconoce la vulnerabilidad crítica de los cables submarinos y la necesidad de reforzar las herramientas de detección y

[111] Ibid.
[112] FRASCÀ, D. y GALANTINI, L. *Op. cit.*
[113] POHORYLES. *Op. cit.*
[114] MUUGA *et al*. *Op. cit.*
[115] SWISTEK y PAUL. *Op. cit.*
[116] BUEGER y LIEBETRAU. *Op. cit.*

atribución, la ausencia de un marco internacional actualizado limita la capacidad de respuesta estatal[117]. Los instrumentos vigentes, como el *Convenio 1884 para la Protección de los Cables Submarinos* y la UNCLOS, no contemplan adecuadamente las amenazas tecnológicas emergentes ni la creciente dimensión estratégica de estas infraestructuras[118].

A ello se suma el aumento de la presión estratégica derivada de la militarización del Ártico, las maniobras rusas en el Báltico y la mayor presencia china en puertos europeos[119].

Ante este contexto, algunos Gobiernos han reclamado respuestas más contundentes. En 2024, un informe del Parlamento británico recomendó ir más allá de la mera atribución pública de sabotajes y explorar medidas preventivas y punitivas adicionales[120].

Sin embargo, la dificultad de atribuir autoría genera un vacío jurídico. Autores como Hartmann plantean revisar el uso del artículo 101 de la UNCLOS sobre piratería, aunque advierten de su incompatibilidad con la atribución estatal. Aun así, el procesamiento individual de responsables podría tener cierto efecto disuasorio, aunque limitado[121].

Desde una perspectiva estructural, la Agencia Europea para la Ciberseguridad subraya que la resiliencia de los cables exige un enfoque multinivel y multinacional, ya que ningún Estado puede proteger por sí solo una red transnacional[122]. Esta realidad ha impulsado una cooperación creciente entre la UE y la OTAN, en la que la primera aporta regulación, financiación y relación con operadores privados, y la segunda capacidades militares, vigilancia avanzada y disuasión[123] [124].

La cooperación UE–OTAN se ha institucionalizado mediante las Declaraciones Conjuntas de 2016, 2018 y 2023, y la creación en 2023 de la Task Force UE–OTAN

[117] HARTMANN, J. *Written evidence 139113*, Parlamento del Reino Unido. 2025. https://committees.parliament.uk/work/1557/unclos-fit-for-purpose-in-the-21st-century/publications/written-evidence/?SearchTerm=hartmann&DateFrom=&DateTo=&SessionId=
[118] *UNCLOSDEBATE.* «Protection of underseas cables in Article 113 in UNCLOS is insufficient considering their critical importance». https://www.unclosdebate.org/evidence/2135/protection-underseas-cables-article-113-unclos-insufficient-considering-their-critical?
[119] BERMINGHAM. *Op. cit.*
[120] 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
[121] Ibid.
[122] ENISA. *Op. cit.*
[123] LOIK. *Op. cit.*
[124] BUEGER, LIEBETRAU y FRANKEN. *Op. cit.*

sobre resiliencia de infraestructuras críticas, que ha formulado recomendaciones en materia de intercambio de información, evaluación de vulnerabilidades y respuesta coordinada a incidentes, con especial atención a los cables submarinos[125] [126].

En el plano operativo y regulatorio, la OTAN ha reforzado la vigilancia del lecho marino, mientras que la UE ha desarrollado instrumentos como el Plan de Acción sobre seguridad de cables (2025), la red MARSUR y el refuerzo del Common Information Sharing Environment (CISE). Estos instrumentos están orientados a mejorar la conciencia situacional, así como la prevención y la respuesta ante incidentes[127] [128].

Los estudios sobre el Báltico coinciden en que los Estados de la región carecen de recursos suficientes para una protección autónoma, por lo que la solución pasa por una combinación de capacidades nacionales y cooperación UE–OTAN, basada en vigilancia, disuasión, regulación y financiación compartidas[129].

En síntesis, aunque persisten lagunas y asimetrías, la protección de los cables submarinos se ha consolidado como uno de los ejes más urgentes y tangibles de la cooperación UE–OTAN frente a amenazas híbridas, especialmente en regiones de alta vulnerabilidad como el mar Báltico[130].

Conclusiones

El análisis realizado confirma la hipótesis planteada: los condicionantes físicos, jurídicos y geopolíticos del mar Báltico convergen para convertir a los cables submarinos en un vector privilegiado de guerra híbrida, frente al cual las capacidades de respuesta de la Unión Europea y la OTAN siguen siendo insuficientes[131].

[125] ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE. «NATO and the EU set up taskforce on resilience and critical infrastructure», *OTAN/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
[126] *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
[127] CONTE DE LOS RÍOS. *Op. cit.*
[128] COMISIÓN EUROPEA. *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
[129] MIĘTKIEWICZ, R. «Hybrid threats in the Baltic Sea: The results of analysis of countermeasure options», *Terroryzm – studia, analizy, prewencja*, edición especial. 2025, pp. 35-71. https://doi.org/10.4467/27204383TER.25.002.21505
[130] BUEGER, LIEBETRAU y FRANKEN. *Op. cit.*
[131] MAULDIN y BUDETTE. *Op. cit.*

La baja batimetría, la densidad de infraestructuras críticas, la accesibilidad del lecho marino y la dificultad de reparación facilitan tanto daños accidentales como hostiles, al tiempo que complican la detección temprana y la atribución concluyente de responsabilidades, difuminando la línea entre lo accidental y lo deliberado[132].

A esto se suma la naturaleza estructuralmente ambigua del dominio marítimo. La ausencia de testigos, la extensión del espacio operativo, la posibilidad de desactivar sistemas de rastreo y las limitaciones técnicas de las investigaciones subacuáticas crean un escenario propicio para operaciones encubiertas[133] [134].

Tal como muestra la literatura sobre guerra híbrida, estas acciones operan deliberadamente por debajo del umbral del conflicto armado y explotan vulnerabilidades estatales mediante tácticas de negación plausible[135] [136]. En el Báltico, esta ambigüedad se intensifica debido al intenso tráfico marítimo, que genera un «ruido estadístico» de incidentes aparentemente accidentales, lo que dificulta demostrar la intencionalidad[137].

La dimensión jurídica refuerza estas conclusiones. Aunque el derecho del mar establece un marco básico, sus lagunas son especialmente visibles en la protección de cables submarinos.

La limitada jurisdicción en la zona económica exclusiva, la dificultad de investigar sabotajes tras la salida de un buque de la jurisdicción costera y la obsolescencia de marcos normativos como el Convenio de 1884 evidencian que los Estados europeos carecen de herramientas suficientes para prevenir, atribuir o sancionar eficazmente actividades híbridas[138]. Por ello, desde Bruselas, Washington y Londres se ha subrayado la necesidad de modernizar los marcos internacionales y reforzar la arquitectura normativa que protege estas infraestructuras críticas[139].

En el plano geopolítico, el Báltico se consolida desde 2022 como un espacio especialmente expuesto a tensiones estratégicas. Su condición cuasi de «lago OTAN»,

[132] BURGER. *Op. cit.*
[133] BERNABÉ *et al*. *Op. cit.*
[134] MUUGA *et al*. *Op. cit.*
[135] OGRYZKO y RIZZI. *Op. cit.*
[136] RID Y BUCHANAN. *Op. cit.*
[137] CAREY. *Op. cit.*
[138] HARTMANN. *Op. cit.*
[139] CONTE DE LOS RÍOS. *Op. cit.*

la militarización rusa en Kaliningrado y la creciente implicación de China en la soberanía digital intensifican la competencia por el control del lecho marino[140].

La combinación de accidentalidad verosímil, intereses contrapuestos y presión estratégica confirma que la vulnerabilidad de los cables es tanto técnica como política[141].

Estos hallazgos muestran que el Báltico es un espacio paradigmático de las dinámicas contemporáneas de guerra híbrida.

Mientras persistan dificultades para atribuir autoría, proteger físicamente el lecho marino, coordinar respuestas multilaterales y dotar de capacidad operativa los marcos existentes, la UE y la OTAN enfrentarán una asimetría estructural frente a actores que operan con costes bajos y efectos estratégicos elevados[142].

Reforzar la resiliencia, actualizar los marcos jurídicos y profundizar la cooperación UE–OTAN emergen, así, como prioridades cruciales para la seguridad europea en las próximas décadas[143].

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

Profesora e investigadora en la Universidad P. Comillas (ICAI-ICADE-CIHS), asesor parlamentario en el Congreso de los Diputados, responsable de programas de Novaindef, analista de comunicación en el Mando de Operaciones, máster en diplomacia y relaciones internacionales, teniente de navío de la Armada

[140] CODREANU. *Op. cit.*
[141] MAULDIN, CONSTABLE, y BURDETTE. *Op. cit.*
[142] BRAW. *Op. cit.*
[143] CONSEJO DE LA UNIÓN EUROPEA Y COMISIÓN EUROPEA. *Op. cit.*