CENTER FOR
CYBERSECURITY
POLICY AND LAW

WHITEPAPER

SHORING UP SUBSEA CABLE SECURITY: A POLICY ROADMAP TO ENHANCE RESILIENCE IN EUROPE

FEBRUARY 2026

Introduction

Subsea cables form the invisible backbone of Europe's digital, energy, and economic security. Approximately 98% of global internet traffic transits through submarine cables, carrying everything from financial transactions and cloud services to government communications and critical infrastructure data.[1]

As geopolitical tensions rise and maritime domains become more contested, the resilience and security of this infrastructure have drawn increasing attention from both governments and industry. This growing concern was reflected in the New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World ("New York Principles"), initially signed by 17 countries in September 2024 and now more than 30 countries, which signaled a shared commitment to protecting undersea cable infrastructure and identified priority areas for international cooperation, including the need to deepen public-private collaboration.[2]

The Center for Cybersecurity Policy and Law's (CCPL) whitepaper, *Shoring Up Subsea Cable Security*, built on this momentum by proposing a global action plan to translate these high-level principles into more concrete policy and operational measures.[3] This paper applies a European lens to those recommendations, noting its dense connectivity, distinctive geographic vulnerabilities, and recent high-profile subsea incidents have elevated submarine cables as a strategic economic and security concern.

Drawing on the original paper's 34 recommendations, this analysis tailors and refines them for the EU landscape, offering region-specific recommendations designed to support European institutions, Member States, and private operators in strengthening the resilience, security, and governance of subsea cable infrastructure cutting across the Union.

EU Landscape

Over the past decade, Europe's subsea cable capacity has expanded rapidly. Total submarine cable capacity connecting EU Member States to one another and to external partners increased from 318 Tbit/s in 2010 to roughly 3,755 Tbit/s by 2024, reflecting broader trends in digitalization and data usage.[4] As capacity has grown, so too has Europe's exposure to the physical constraints of its maritime geography.

---

[1] European Commission, Report on Security and Resilience of EU Submarine Cable Infrastructures, October 23, 2025, pg. 6, digital-strategy.ec.europa.eu/en/library/report-security-and-resilience-eu-submarine-cable-infrastructures.

[2] European Commission, The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World, September 26, 2024, https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world.

[3] Center for Cybersecurity Policy and Law (CCPL), Shoring Up Subsea Cable Security, September 24, 2025, www.centerforcybersecuritypolicy.org/insights-and-research/shoring-up-subsea-security-a-comprehensive-action-plan-to-promote-submarine-cable-resiliency-security-governance.

[4] European Commission, *EU Submarine Resilience Report*, pg. 9.

The EU hosts more than 300 submarine cable landing stations, yet traffic remains concentrated around a limited number of strategic chokepoints. The Red Sea corridor, for example, carries an estimated 90% of data traffic between Europe and Asia, making it a critical global bottleneck.[5] Within Europe, several major landing hubs, such as Marseille and Sines, have invested in geographic redundancy, but others remain vulnerable to disruption. Island Member States, including Ireland, Cyprus, and Malta rely almost exclusively on submarine cables for international connectivity, leaving them particularly exposed to cable damage or prolonged outages. In Northern Europe, dense networks of cables connect closely situated states across shallow waters, increasing both redundancy and the likelihood of interaction with maritime activity.

It is important to note that most submarine cable incidents globally, and in Europe, are unintentional, caused by fishing activity, anchoring, dredging, or natural phenomena such as seabed movement and undersea currents.[6] Industry data shows that the global number of cable faults has remained broadly stable over the past five years, while Europe has actually experienced a decline in reported incidents by 7% year-over-year, and in Northern Europe faults have decreased by nearly 30% since 2020.[7] This is despite an increase in the number of cable kilometers in operation. The fault rate has decreased from 1 per 5,173 km in 2015 to 1 per 8,759 km in 2024.[8] These improvements are attributed to better cable burial practices, improved cable design, enhanced engagement with fishing communities, and the retirement of older, shallow-water cables that were particularly vulnerable.

Operationally, Europe benefits from a relatively robust submarine cable repair ecosystem, defined not only by the availability of maintenance vessels but also by the regulatory frameworks that allow those vessels to operate. Over the past four years, there has been on average only one incident per year in which a repair vessel could not be mobilized within 24 hours due to competing repair demands. [9] In the Baltic Sea, maintenance providers have consistently been able to respond within 24 hours for unrepeated cables, reflecting both the availability of vessels and the presence of long-term repair permits that allow operators to act without seeking case-by-case authorization. Under normal conditions, this combination has enabled relatively rapid repair timelines. However, this margin is thin.

Forecasts indicate that the number of cable faults in Europe could rise by more than 25% by 2035, driven by increased cable density, higher maritime traffic, and expanding offshore infrastructure. [10] Any reduction in the number of maintenance vessels, or delays caused by fragmented or slow permitting processes, particularly in the Atlantic and Mediterranean, where access to territorial waters can take from several days

---

[5] Ibid., pg 12.

[6] International Cable Protection Committee, Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunication Cables, (last accessed Feb. 5, 2026), ICPC-Gov't-Best-Practices-for-Cable-Protection--Resilience-Version-1.2-(English)%20(9).pdf.

[7] European Commission, *EU Submarine Resilience Report*, pg. 10.

[8] International Cable Protection Committee, Global Cable Repair Data Analysis, 2025.

[9] European Commission, *EU Submarine Resilience Report*, pg. 11.

[10] Telegeography, *The Future of Submarine Cable Maintenance Trends, Challenges, and Strategies*, 2025, www2.telegeography.com/future-submarine-cable-maintenance-report.

to four weeks, could significantly extend repair times and amplify economic impact.[11] These dynamics highlight that repair capacity in Europe depends as much on regulatory readiness as on physical assets, and that permitting disparities represent a latent vulnerability in crisis scenarios.

Threat Environment

In recent years, a series of high-profile incidents in the Baltic Sea and beyond has heightened political and operational attention toward subsea infrastructure. While many cases have involved unintentional damage linked to maritime activity, several high-profile events have underscored how difficult it can be to distinguish accidents from intentional interference.

In October 2023, the container ship *NewNew Polar Bear* damaged the Balticconnector gas pipeline between Finland and Estonia, along with three submarine telecommunications cables, after dragging its anchor across the seabed.[12] The incident demonstrated how a single vessel could disrupt multiple forms of critical infrastructure simultaneously. Concerns intensified in late 2024, when the BCS East-West Interlink cable between Sweden and Lithuania was cut, followed less than 24 hours later by damage to the C-Lion1 telecommunications cable connecting Finland and Germany.[13] One month later, the Estlink 2 power cable between Finland and Estonia was severed, reducing cross-border electricity capacity by nearly 70%. Finnish authorities detained the oil tanker *Eagle S,* suspected of operating as part of a Russian-linked shadow fleet, and later brought charges against its officers.[14]

Additional incidents in 2025, including damage to cables between Sweden and Latvia and the seizure of vessels suspected of causing cable breaks in Finnish waters, reinforced concerns about recurring risks in the Baltic Sea.[15] Collectively, these events reveal a spectrum of cause and have sharpened awareness across EU capitals of the vulnerability of submarine infrastructure to grey-zone activity, hybrid threats, and the challenges of monitoring and attribution in a congested maritime domain.

Legislative Responses

Against this backdrop of rising geopolitical tension and repeated subsea incidents, the European Union has moved to formalize its response, advancing legislation and strategic frameworks that explicitly recognize submarine cables as critical infrastructure requiring enhanced protection and oversight. At the legislative

---

[11] European Commission, *EU Submarine Resilience Report*, pg. 12.

[12] AP News, 'Anchor of Chinese container vessel caused damage to Balticconnector gas pipeline', October 24, 2023, apnews.com/article/finland-estonia-china-vessel-baltic-sea-gas-pipeline-39334c9c565753c7e189c6efc302e43e.

[13] Submarine Cable Networks, 'C-Lion1 breaks in the Baltic Sea', November 19, 2024, www.submarinenetworks.com/en/systems/intra-europe/sea-lion/c-lion1-breaks-in-the-baltic-sea

[14] Submarine Cable Networks, 'Finland charges Russian-linked ship officers over Baltic Sea cable sabotage', August 13, 2025, www.submarinenetworks.com/en/nv/insights/finland-charges-russian-linked-ship-officers-over-baltic-sea-cable-sabotage.

[15] BBC, 'Finnish police seize ship suspected of sabotaging undersea cable', December 31, 2025, www.bbc.com/news/articles/c62040np372o.

and policy level, the EU has progressively assembled a framework aimed at strengthening the resilience and security of submarine cable infrastructure:

- **EU Action Plan on Cable Security (February 2025):** Adopted by the European Commission and the High Representative for Foreign Affairs and Security Policy, the Action Plan establishes a coordinated approach to protecting telecommunications and power submarine cables.[16] It spans the full resilience cycle from prevention, detection, response, recovery, and deterrence, and places particular emphasis on situational awareness, cross-border coordination, and preparedness for hybrid and grey-zone threats.
    - **Cable Security Toolbox (February 2026):** Outlines six strategic and four technical and support measures to improve the security of submarine cable infrastructure, building on the October 2025 risk assessment discussed below.[17]
    - **Cable Projects of European Interest (February 2026):** List of 13 CPEI areas for public funding specifies three five-year stages, up to 2040, to fund projects aimed at strengthening the resilience of submarine cables. CPEI areas will be prioritized for funding under Connecting Europe Facility (CEF) Digital calls for proposal and will inform planning for possible future funding.[18]
- **Commission Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures:** This Recommendation focuses specifically on data cables and calls on Member States to improve mapping of existing and planned infrastructure, conduct comprehensive risk assessments, and strengthen cooperation between public authorities and private operators.[19]
- **Council Recommendation on Critical Infrastructure Resilience (2022):** Provides the overarching framework for a Union-wide, coordinated approach to strengthening the resilience of critical infrastructure, including subsea assets.[20]
- **NIS 2 Directive:** Expands cybersecurity obligations for operators of essential services and digital infrastructure, reinforcing requirements related to risk management, incident reporting, and supply-chain security.[21] In an amendment of the Directive proposed in February 2026, a reference to submarine infrastructure is added, confirming and streamlining coverage by the NIS2 framework.

---

[16] European Commission, *EU Action Plan on Cable Security*, February 21, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009.

[17] EU Expert Group under Recommendation 2024/779 on Secure and Resilience Submarine Cable Infrastructures, *Submarine Cable Security Toolbox and Cable Projects of European Interest*, February 5, 2026.

[18] Ibid.

[19] European Commission, *Commission Recommendation (EU) 2024/79 on Secure and Resilient Submarine Cable Infrastructures*, February 26, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400779.

[20] The Council of the European Union, *Council Recommendation 2023/C 20/01 on a Union-Wide coordinated approach to strengthen the resilience of critical infrastructures*, December 8, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2023_020_R_0001.

[21] European Commission, 'NIS2 Directive: securing network and information systems' January 20, 2026, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

- **Critical Entities Resilience (CER) Directive:** Introduces binding obligations for Member States and operators to identify critical entities, assess risks, and implement resilience measures across key sectors, including those dependent on subsea connectivity.[22]

In addition, the *proposed* Cybersecurity Act (CSA) 2.0 aims to enhance the security of the EU's information and communication technology (ICT) supply chains and will establish a trusted ICT supply chain security framework based on harmonized, risk-based approach. It will enable the mandatory derisking of the European telecommunication networks from high-risk vendors, building on the work being carried out under the 5G security toolbox.[23] Likewise, the Proposed Digital Networks Act introduces regulatory measures aimed at strengthening the resilience and preparedness of EU communication networks.[24]

To support implementation of the 2024 Recommendation, the Commission established the Submarine Cable Infrastructures Expert Group, composed of Member State authorities and the EU Agency for Cybersecurity (ENISA). The group was mandated to: consolidate national mapping exercises into an EU-level overview of existing and planned submarine cable infrastructure; conduct a Union-wide assessment of threats, vulnerabilities, and dependencies; and propose a list of Strategic Cable Projects of European Interest to guide prioritization and investment.[25] In October 2025, the Expert Group delivered a comprehensive report and risk assessment on the security and resilience of EU submarine cable infrastructure, including stress-testing scenarios and cross-border risk analysis, representing the most detailed assessment conducted at Union level to date.[26] In February 2026, the Expert Group delivered the Subsea Cable Security Toolbox and Cable Projects of European Interest.

Operational, Financial, and Security Responses

Beyond legislation, the EU and its partners have pursued a range of operational, financial, and security-focused measures to translate policy objectives into practical resilience.

A key financial instrument includes the Connecting Europe Facility (CEF) Digital Programme, under which €1.5 billion has been earmarked from the EU's 2021–2027 budget to support digital connectivity projects. To date, a total of €533 million is allocated for submarine cable projects, with €186 million already awarded to 25 projects. This includes €35.6 million invested in eight submarine data cable projects in the Atlantic, Nordic, and Baltic regions. An additional €540 million is scheduled for investment between 2025 and 2027, with a focus on digital infrastructure projects incorporating "smart" technologies, such as sensors and

[22] The European Parliament and the Council of the European Union, *Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, December 14, 2022, https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[23] European Commission, Proposal for a Regulation for the EU Cybersecurity Act, January 20, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act.

[24] European Commission, Proposal for a Regulation for the Digital Networks Act, January 21, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna.

[25] European Commission, 'EU improves Submarine Cable Security and Resilience', March 16, 2024, https://ec.europa.eu/newsroom/cipr/items/822835/.

[26] European Commission, *EU Submarine Resilience Report.*

monitoring systems, that can act as early warning mechanisms for potential threats.[27] These investments align closely with the objectives of the EU Action Plan on Cable Security and prioritize Strategic Cable Projects of European Interest, including those supporting the EU's Global Gateway connectivity with third countries.

The EU has also intensified regional and international cooperation. In April 2024, six North Sea countries, Belgium, Denmark, Germany, the Netherlands, Norway, and the United Kingdom, committed to enhanced information sharing to improve protection of critical submarine infrastructure.[28] In the Baltic Sea region, this momentum continued with the signing of a Memorandum of Understanding in May 2025 between the EU, eight Member States, Norway, and Iceland under the Council of the Baltic Sea States, aimed at strengthening coordination on the protection of undersea infrastructure.[29]

At the security and defense level, NATO has complemented EU efforts through the launch of Baltic Sentry, announced in January 2025 at a summit of Baltic Sea Allies in Helsinki.[30] The initiative enhances NATO's military presence in the Baltic Sea and aims to improve allies' ability to deter and respond to destabilizing acts targeting critical undersea infrastructure. NATO has also committed to working with industry through its Critical Undersea Infrastructure Network to improve situational awareness and resilience.

Finally, the EU has sought to anchor its approach within a broader international framework. In September 2024, the Union formally endorsed the New York Principles for the Security and Resilience of Undersea Cables[31], and in March 2025, G7 Foreign Ministers underscored the importance of submarine cables and reaffirmed the UN Convention on the Law of the Sea as the foundation of maritime governance.[32] These initiatives reflect recognition that effective protection of subsea infrastructure will depend upon international norms and cooperation.

---

[27] European Commission, 'Joint Communication to strengthen the security and resilience of submarine cables', February 21, 2025, digital-strategy.ec.europa.eu/en/factpages/joint-communication-strengthen-security-and-resilience-submarine-cables.

[28] AP News, '6 northern European nations sign a deal to protect North Sea infrastructure from hostile actors', April 9, 2024, https://apnews.com/article/north-sea-infrastructure-threats-denmark-a97a3e7837c4bafd0fd1a4c85f559056.

[29] Government Offices of Sweden, 'Sweden signs Memorandum of Understanding on the protection of critical undersea infrastructure', May 21, 2025, www.government.se/press-releases/2025/05/sweden-signs-memorandum-of-understanding-on-the-protection-of-critical-undersea-infrastructure/.

[30] NATO, 'NATO launches Baltic Sentry to increase critical infrastructure security', January 14, 2025, www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security.

[31] European Commission, *The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World,* September 26, 2024, https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world.,

[32] G7, 'G7 Foreign Ministers' Declaration on Maritime Security and Prosperity', March 14, 2025, https://g7.canada.ca/en/news-and-media/news/g7-foreign-ministers-declaration-on-maritime-security-and-prosperity/.

Our Recommendations

Against this threat environment and evolving legislative landscape, the following recommendations aim to support the European Union in strengthening the resilience, security, and governance of its submarine cable infrastructure. Because submarine cable systems are inherently global, and each cable may connect multiple jurisdictions, Europe's cable security is inseparable from the security of the broader international subsea network. Strengthening EU resilience therefore requires measures that reinforce not only regional protections, but also cooperation and risk mitigation across the global cable ecosystem.

Ecosystem Resilience

1. Governments and industry should jointly strengthen contingency planning for submarine cable repair capacity, ensuring that existing industry-led maintenance models are preserved while establishing clear mechanisms to mobilize additional public or dual-use maritime assets in the event of simultaneous or large-scale disruptions.

2. Governments should streamline and harmonize regulatory and permitting frameworks for cable installation, maintenance, and repair across EU maritime basins, in coordination with international partners, drawing on best practices such as multi-year repair permits in the Baltic Sea. This approach should aim to reduce delays and ensure rapid restoration of service under both routine and crisis conditions. It would also promote consistency with allied regulatory regimes to avoid fragmented or bespoke subsea cable requirements across regions.

3. Governments and industry should establish and/or strengthen trusted, two-way mechanisms for sharing risk, incident, and intelligence data across the maritime and subsea supply chain, incorporating cable operators, developers, vendors, and other key stakeholders. Where such mechanisms do not already exist, governments should work collaboratively with industry to create them, while supporting targeted awareness and education efforts to improve situational awareness, identify protection gaps, enable early warning of emerging risks, and support attribution and prosecution of negligent or malicious activity by state and non-state actors.

4. Governments and industry should co-develop a strategy for emergency cable repair capacity, to enable additional government resources to be deployed in the event of a widespread disruption to cables.

Infrastructure Security

5. Governments should strengthen the enforcement of mandatory AIS usage, ensuring consistent application across EU Member States and, in coordination with international partners, improving the ability of maritime authorities to identify vessels operating near submarine cable routes, including those engaging in AIS manipulation or disabling.

6. Governments should explore making the use of VMS tracking mandatory within their EEZ, particularly in regions such as the Baltic Sea, to enhance visibility of activity near submarine cables, and enforcement of negligent activities.

Legal and Institutional Frameworks

7. Governments should ensure that coast guards and law-enforcement authorities are familiar with submarine cable protection laws and work closely with operators to investigate cable damage, while establishing and consistently enforcing proportionate penalties for vessels and responsible parties that cause damage through negligence or unlawful activity. This should be supported by clear liability frameworks and coordinated investigative procedures across EU Member States to strengthen accountability and deterrence.

8. Governments should increase inspections of ships and impose penalties for noncompliance with safety standards, in order to deter risky maritime practices and help reduce the number of accidental cable breaks.

9. Governments should ensure that charting authorities update nautical charts regularly, showing all submarine cables, and all other human activities that could pose risks to them.

10. Governments should leverage existing EU, regional, and allied security cooperation mechanisms to conduct coordinated patrols and surveillance in high-risk maritime areas, and to facilitate timely intelligence sharing related to potential threats to submarine cable infrastructure.