BRIEFING NOTE No. 208

Troubled waters: Europe's subsea telecommunications network

March 2026

By Sasha Pearson

Summary

Subsea telecommunication cables are the digital arteries of the modern world. Carrying more than 95% of global data traffic, these cables are the invisible backbone of Europe's digital economy. Yet the ownership and operational control of this infrastructure are quietly shifting, with far-reaching implications for Europe's economic resilience, strategic autonomy, and digital sovereignty objectives.

Although high-profile sabotage incidents and concerns about hybrid threats have dominated media and policy discussions, they risk overshadowing more profound structural challenges. Fragmented governance among national authorities and EU institutions results in a lack of a comprehensive overview or mandate. Additionally, a small number of US hyperscalers - Amazon, Google, Meta and Microsoft - now control a growing share of global capacity and operational control, while increasing financial pressures are eroding the competitive position of European operators.

The core challenge for Europe's subsea network, therefore, extends beyond the immediate risk of hybrid attacks: it lies in the gradual transfer of ownership and control of this critical infrastructure to non-EU actors. This consolidation fosters structural dependencies that threaten to erode Europe's capacity to shape its own digital future. Addressing these risks requires moving beyond reactive security measures toward a coordinated European strategy grounded in governance reform, industrial policy, and strategic investment.

Introduction

Contrary to popular imagination, the internet does not float in the cloud. It runs along the ocean floor. Subsea telecommunications cables - often no thicker than a garden hose - carry the vast majority of the world's international data traffic. These fibre-optic cables underpin everything from financial markets to government communications. For Europe, the continent with the highest number of cable landings, this infrastructure is a critical foundation of its economic competitiveness, resilience, and autonomy.

Yet the strategic importance of Europe's subsea infrastructure only recently found its way onto the policy agenda. Concerns about hybrid threats following Russia's invasion of Ukraine, combined with a string of high-profile sabotage incidents, sharpened policymakers' attention. The initial response has focused on security - prevention, detection, response, and repair. While necessary, these measures address only one dimension of the challenge currently facing the network.

Beneath the surface lie deeper structural vulnerabilities - ones that bear directly on the union's quest for digital sovereignty and strategic autonomy. These stem from three distinct yet mutually reinforcing dynamics: fragmented governance and weak EU-level oversight; the rapid expansion of hyperscalers into cable ownership, capacity management, and investment; and mounting financial pressure on European telecommunications operators.

Europe has long been a central player in the global subsea cable industry; however, that position is now under pressure. The rapid vertical integration of US hyperscalers into the sector is transforming its economic foundations, concentrating control of critical data flows in the hands of non-EU actors and exposing Europe to strategic decisions made outside its regulatory reach. This trend raises concerns about weaponised interdependence - and sits within a broader, intensifying debate about digital sovereignty and technological independence. Subsea cables represent one of the latest, and potentially most consequential, frontiers of that challenge.

Addressing this challenge will require a coherent European strategy integrating governance reform, industrial policy, and strategic investment.

1. The threat is real - but mischaracterised

Recent sabotage incidents have exposed the vulnerability of subsea infrastructure - even in deep, heavily monitored waters. On 26 September 2022, the Nord Stream 1 and 2 gas pipelines were sabotaged in the exclusive economic zones of Denmark and Sweden, rupturing and leaking gas into the Baltic Sea. Less than a year later, on 8 October 2023, the Balticconnector gas pipeline linking Finland and Estonia was severed, and two telecommunications cables connecting the same countries were cut simultaneously. Since then, EU policy attention has been intensely focused on the physical security and resilience of subsea cable networks.

Yet the clamour these incidents provoked, across both media and policy circles, has obscured the risk landscape. The statistical reality is that the overwhelming majority of cable faults are caused not by state actors but by commercial fishing vessels and anchors. According to the International Cable Protection Committee (ICPC), ship anchor damage remains a leading cause of damage globally, and in contrast to the above-mentioned cases, most incidents are, in fact, accidental.

Heightened security concerns have simultaneously underscored the critical importance of repair and maintenance capabilities. With only 63 cable ships active globally[1], these highly specialised vessels - essential for repair, maintenance, and the installation of new systems - are vital but scarce. The current fleet is ageing, and estimates suggest that between €225 million and €330 million in capital expenditure will be required over the next 10 to 15 years to maintain the European fleet at its current size. Securing adequate financing remains a significant challenge despite Europe's strong industrial capacity in the maintenance and repair sector.

Box 1: European industrial ecosystem

Europe retains strong industrial and operational capabilities in the subsea cable sector, underpinned by several European champions with genuine global reach. Political attention on the cable sector has translated into direct state intervention: at the end of 2024, the French government acquired Alcatel Submarine Networks (ASN) from Nokia, while in April 2025, a consortium led by the Italian Ministry for the Economy and Finance took over Telecom Italia's subsea cable unit, Sparkle.

Suppliers:
ASN is the leading global supplier. Between 2021 and 2025, the company supplied 23 cable systems, produced 174,470 km of cable and installed 25 systems[2] - a scale that no competitor comes close to matching. Italy's Elletra occupies a strong mid-tier position, producing 65,770 km of cable over the same period, though its involvement in only two installations reflects a focus on larger, more complex projects rather than volume.

Installation and repair:
European leverage extends well beyond manufacturing. ASN accounted for 29.1% of global system installations between 2021 and 2025; Orange Marine, the other major French player, delivered a further 12.8% - eleven systems in total. Both companies operate fleets of six cable ships each, giving Europe an independent capacity for deployment and repair.

Operators:
Manufacturing and installation tell only part of the story. Operators such as Sparkle, Orange and GlobalConnect are equally critical: they shape route diversification, underpin network resilience and determine where data flows. Sparkle, with a global fibre network exceeding 600,000 km, has actively promoted alternative cable routes designed to enhance resilience and bypass strategic chokepoints. Orange manages over 450,000 km of subsea cables connecting all continents - a footprint that extends its role well beyond installation and repair.

Europe's subsea ecosystem also features a tier of important specialist players: Italy's Prysmian Group, France's Nexans and Sweden's Hexatronic each play a supporting role in regional and specialised systems.

Source: Author

2. The emerging European policy architecture

Since 2024, the European Union has begun developing a policy framework for subsea cables, moving beyond fragmented commercial oversight toward a more coordinated approach to infrastructure security and resilience. The architecture, however, remains at an early stage of implementation.

The European Commission's 2024 Recommendation on the security and resilience of subsea cables and the subsequent 2025 EU Action Plan established the first coordinated approach to subsea infrastructure protection at the Union level. Acting as foundational blueprints, these initiatives have played a crucial role in fostering technical alignment among Member States, the EU Agency for

Cybersecurity (ENISA), and NATO, whilst integrating subsea cables into the EU's horizontal security landscape[3] for securing critical infrastructure.

To support this effort, the Submarine Cable Expert Group[4] has undertaken an EU-wide mapping of the network, along with comprehensive risk assessment and stress-test guidance for member states. In February 2026, the group delivered the 'Cable Security Toolbox', providing strategic and technical measures to enhance resilience, incident preparedness, prevention, and monitoring. At the same time, the EU identified 13 priority areas for Cable Projects of European Interest[5] (CPEIs), signalling growing recognition of the strategic importance of subsea connectivity.

Financial support has also increased. Through the digital component of the Connecting Europe Facility (CEF Digital), the EU has allocated more than €420 million[6] to backbone connectivity projects, with an additional €347 million announced in early 2026 for strategic submarine cable initiatives, along with a €20 million call focusing on faster cable repairs. Submarine cables are also a priority of the EU Global Connectivity Strategy, the Global Gateway, which aims to increase European investments in developing and emerging economies, aided by a combination of grants from the European Commission (DGs INTPA, MENA, ENEST) and loans from EIB Global, EBRD and other European development banks.

These policies and measures represent meaningful progress, and the scope of EU analysis of the problems has broadened considerably since the initial recommendation. Yet actionable policy continues to lag behind rhetoric. Addressing the deeper structural vulnerabilities of Europe's subsea ecosystem will require policymakers to move beyond physical protection - toward enhanced governance, strategic ownership, and stronger investment.

3. Fragmented governance and oversight

European subsea governance remains fragmented, characterised by a patchwork of national frameworks and limited cross-border coordination. National approaches diverge significantly: France integrates cable security directly into its state apparatus, whereas Denmark delegates the security of cable protection zones almost entirely to the private sector. This uneven landscape has both operational and strategic consequences, creating significant regulatory burdens for companies operating across multiple jurisdictions while severely limiting the EU's ability to oversee the network as a whole.

Fragmented regulation and procedural constraints have historically caused severe delays in repair operations, while geopolitical tensions increasingly

complicate decisions related to cable laying, maintenance, and repair. The absence of a coordinated European oversight framework is therefore not a mere technical limitation. It represents a structural vulnerability at the core of the Union's critical infrastructure governance.

This fragmentation has also produced a significant information gap. Europe lacks reliable, centralised data on who owns its subsea cables, who is investing in them, and how traffic flows across the network. Policy is only beginning to catch up: while the Submarine Cable Expert Group has warned that deepening dependencies pose a direct threat to the Union's technological sovereignty and economic security, no mandatory reporting requirements are yet in place. By contrast, the United States mandates granular reporting on every landing cable through the Federal Communications Commission (FCC). Europe, therefore, cannot fully account for who owns, funds, or exerts strategic influence over the cables on which its connectivity depends.

4. Hyperscaler consolidation and emerging vulnerabilities

Hyperscalers' expanding involvement in subsea infrastructure - through investment, cable ownership, and capacity consolidation across European networks - raises several strategic concerns for Europe. In particular, these relate to capacity access, infrastructure governance, and structural dependency. Hyperscalers are no longer simply major purchasers of bandwidth; they increasingly design, finance, and in some cases own the cable systems.

Over the past decade, the total share of capacity has shifted decisively away from European operators. Google, Meta, Microsoft, and Amazon now collectively control around 90% of capacity on the transatlantic route and about 71% of global subsea fibre capacity. Europe's infrastructure is also ageing: the oldest 91 cables - largely carrying public telecom traffic - account for just 2% of capacity, while 74% is concentrated in the newest 31 systems. As hyperscalers increasingly pursue sole-ownership models for new high-capacity cables, which are privately owned and largely unregulated, public authorities have diminishing influence over capacity management and allocation. European operators are left facing growing uncertainty over long-term, affordable access to next-generation infrastructure.

This shift reflects a broader structural transformation in global connectivity infrastructure. Driven by rapid growth in AI data flows, edge computing, and high-density cloud workloads, hyperscalers are increasingly pursuing vertical integration across the digital stack. Instead of relying on external networks that

they cannot fully control in terms of optimisation, pricing, or security, they are turning to direct private ownership of subsea infrastructure as a more efficient and strategically advantageous alternative.

While hyperscaler investment in subsea cables has expanded global connectivity capacity, it has also consolidated control. New cable systems are designed around hyperscaler traffic requirements and data-centre interconnection needs, departing from earlier industry models in which telecommunications carriers jointly financed shared infrastructure through consortium arrangements.

Amid growing uncertainty about the transatlantic partnership's reliability, Europe's increasing dependence on hyperscaler-controlled subsea capacity raises serious questions about the resilience of its connectivity infrastructure. The concentration of cable ownership and traffic management creates real uncertainty over the routing and prioritisation of European data flows - particularly in periods of heightened geopolitical tension. Deliberate disruption is unlikely, but there is no guarantee that European traffic would be prioritised in a crisis, and both cable ownership and capacity management could be used as instruments of leverage.

Beyond issues of control and governance, hyperscaler market disruption is also fundamentally reshaping the market in which traditional European telecommunications operators must compete.

5. The 'squeeze' on European operators

The transformation of the global subsea cable market is placing increasing pressure on private-sector actors in the industry, especially telecom operators. Many European carriers continue to operate within business models built around wholesale capacity markets and shared consortium investment structures. Operators are now caught in a triple squeeze: intensifying market dynamics, a chronic financing gap, and an increasingly securitised environment that treats commercial operators as de facto security entities.

Traditional consortium models, where carriers share risk and financing across joint cable systems, are gradually being replaced by closed, demand-driven network structures. This shift places European operators in a challenging strategic position. Constrained balance sheets limit their ability to finance large-scale deployments independently, while declining participation in new systems risks reducing their long-term influence over future network development.

At the same time, hyperscaler-backed routes tend to focus on high-capacity transcontinental corridors where demand is concentrated. Consequently, strategically important projects - such as those enhancing redundancy, connecting peripheral regions, or diversifying geopolitical risk - face weaker commercial incentives. As a result, many routes of significant strategic value struggle to attract sufficient private investment.

Bridging this investment gap is critical for ensuring Europe's continued access to global connectivity and will increasingly necessitate public-sector support or risk-sharing mechanisms. Ensuring long-term access through adequate investment is particularly pressing given the rise of hyperscaler-led sole-ownership cable projects: Meta's Project Waterworth, for instance, bypasses Europe entirely.

Whilst EU instruments have sought to address market failures in strategic connectivity projects, the scale of support remains modest relative to the capital intensity of modern cable systems. While initiatives like CEF Digital and Global Gateway have increased financial support, the expert group estimates that delivering the 13 priority areas of Cable Projects of European Interest would require more than €10 billion. Against this backdrop, the additional €347 million CEF allocation to fund strategic submarine cable projects, while welcome, remains limited in scale.

Furthermore, financing mechanisms remain fragmented,[7] bureaucratic, and slow relative to commercial timelines. The experience of the Medusa cable system, a Global Gateway flagship initiative, illustrates this clearly: due to its strategic relevance, the project benefited from a CEF grant and an additional grant from then DG NEAR, but has not been able to secure EIB financing thus far. This case demonstrates a gap between political ambition and delivery capacity.

More broadly, the EIB remains underutilised as a strategic financing actor, constrained by its limited HR capacities and risk appetite. Without a more coordinated, scaled, and market-aligned financing approach, European operators may be pushed to seek non-EU capital, which - when provided through equity investment - can raise additional concerns for Europe's digital sovereignty.

Europe's research and education network, GÉANT, demonstrates how coordinated demand aggregation can secure long-term international connectivity without requiring direct ownership of subsea infrastructure.

Box 2: GÉANT: Securing sovereign lanes

The GÉANT network coordinates connectivity for Europe's national research and education networks, pooling their requirements to secure long-term access to international fibre and subsea capacity. Supported by European Commission funding through the CEF Digital and financing from EIB, this approach enables strategic access to connectivity infrastructure without requiring full ownership of cable systems.

Two initiatives illustrate this approach. Through the BELLA programme, GÉANT and its regional partner RedCLARA secured 25-year capacity on the EllaLink submarine cable linking Portugal and Brazil, ensuring dedicated transatlantic connectivity for research networks. Similarly, within the Global Gateway flagship project Medusa, GÉANT is supporting the integration of research institutions across North Africa into Europe's research network, securing long-term high-capacity connectivity through coordinated demand.

While not easily replicated in commercial markets, the model demonstrates how coordinated demand and targeted public support can secure long-term access to strategically important connectivity infrastructure. Nevertheless, dependency on system operators and owners within privately owned cable systems remains a potential risk.

Source: Author

The evolving securitised environment has placed additional operational expectations and burdens on European commercial cable operators. Regulatory frameworks such as the NIS2 Directive and the CER Directive require operators to strengthen the protection of both digital and physical infrastructure from sabotage and natural hazards alike. The Cable Security Toolbox further encourages measures such as maritime monitoring, vessel tracking, advanced threat detection technologies, reinforced cable armouring, and the hardening of landing stations. Each of which requires significant capital. By shifting these responsibilities onto the private sector, the EU effectively outsources the protection of its critical communications infrastructure, expecting commercial actors to defend the Union's digital nervous system without the strategic coordination, defence funding, or state-backed commitments that typically underpin national security responsibilities.

Together, these dynamics create an increasingly challenging operating environment for European telecommunications firms. Operators must compete in an increasingly concentrated global market while simultaneously assuming

greater responsibilities for infrastructure security and resilience. Without stronger coordination among industrial policy, infrastructure investment, and security regulation, there is a risk that European operators historically central to the subsea ecosystem will play a diminishing role in shaping the continent's future connectivity architecture.

Conclusion

Subsea cables are not merely communications infrastructure - they are strategic assets, and Europe's control over them is weakening. The sabotage incidents that first drew policymakers' attention to this network have obscured deeper structural challenges.

These challenges are threefold: governance remains fragmented; hyperscaler consolidation is concentrating control of critical data flows in the hands of non-EU actors; and the financing architecture needed to sustain European industrial capacity remains inadequate and misaligned with commercial realities. Taken together, these dynamics risk producing an outcome in which Europe retains the ambition of digital sovereignty but progressively surrenders control of the infrastructure on which it depends.

More subsea data cables connect to Europe than to any other continent, and Europe retains world-leading industrial capability in this domain. The institutional architecture is now substantially in place. What is missing is the coherence to translate security ambition into structural industrial resilience. Closing that gap, and not merely cataloguing threats, is the policy work that most urgently remains undone.

Recommendations: A more coherent path forward

Europe's subsea cables will not be secured solely by threat perception. What is required is a strategy that functions simultaneously as a security strategy, an industrial strategy, and a digital sovereignty strategy - and that recognises these objectives as mutually reinforcing rather than in tension. Addressing Europe's structural vulnerabilities will require governance reform, more coherent investment frameworks, and closer cooperation between public authorities and industry.

1. Establish a European subsea cable governance authority

Europe currently lacks a permanent institutional structure to oversee the subsea cable ecosystem. Governance remains fragmented across national administrations, with limited coordination at the EU level and no single body

responsible for maintaining a comprehensive view of network infrastructure and dependencies. **The EU should therefore establish a dedicated European Subsea Cable Governance Authority responsible for regulatory oversight, operational data collection, and coordination between Member States, the European Commission, ENISA, and industry.** Such a body would maintain a centralised map of cable systems and landing stations, coordinate risk assessments and crisis response, and provide a permanent institutional focal point to ensure coherence between industrial policy, infrastructure investment, and security regulation.

2. Mandate ownership and capacity transparency

The EU should introduce binding reporting requirements for subsea cable infrastructure, modelled on the U.S. Federal Communications Commission's framework. One of the key governance gaps in Europe's subsea ecosystem is the lack of systematic visibility over cable ownership, capacity allocation, and investment structures. Mandatory reporting for all EU landing stations should require disclosure of ownership arrangements, capacity distribution, financing structures, and operational incidents. Data should be maintained through a centralised European registry accessible to regulators and policymakers. Improving transparency would allow the EU to track shifts in infrastructure ownership, identify emerging dependencies, and better monitor control over international connectivity in an increasingly concentrated market.

3. Consolidate and coordinate EU financial instruments.

Europe's financing landscape for subsea cable infrastructure remains fragmented, slow, and modest. Routes typically require investments of €300-500 million. Yet, support mechanisms across CEF Digital, EIB, and Global Gateway operate in silos, with bureaucratic timelines that struggle to match the speed of commercial deployment. **The EU should consolidate and better coordinate existing instruments. This means streamlining grant and loan guarantee mechanisms under CEF Digital, expanding EIB lending capacity for strategic connectivity projects (including HR capabilities), and establishing clearer pathways for operators to access combined financing.** There are tentative signs of progress: the Commission's CPEI framework identifies areas that will inform future CEF Digital funding calls, with proposals addressing these areas to be prioritised within the applicable selection rules. Furthermore, the proposed ECF instrument offers a potential vehicle for enhanced coordination. Critics caution, however, that its operational parameters remain too vague to assess - and without clear governance structures and deployment timelines, it risks replicating the fragmentation it seeks to address. Without stronger coordination and

financing, European operators risk growing dependence on non-EU capital, further eroding Europe's control over its own connectivity infrastructure.

4. Realign industrial and security policy

Europe's regulatory frameworks place growing security obligations on telecommunications operators - yet public policy has not kept pace with the costs this entails. NIS2, the CER Directive, and the Cable Security Toolbox require operators to implement extensive resilience measures, imposing significant operational and financial burdens on private actors who are, in effect, performing functions of strategic public importance. Regulation alone is insufficient. **The EU should treat telecommunications operators as strategic security partners and introduce targeted instruments - co-financing mechanisms, risk-sharing arrangements, or public guarantees - to offset the costs of protecting critical connectivity infrastructure.** If operators are expected to shoulder strategic responsibilities, public support should follow.

5. Strengthen public–private cooperation in subsea infrastructure security and planning

Most of Europe's subsea cable infrastructure is owned and operated by private actors, yet the mechanisms for structured dialogue between industry and public authorities remain weak and fragmented. NIS2 and the CER Directive provide a partial basis for coordination but operate primarily through national competent authorities and do not create a permanent cross-sectoral forum at the EU level. **The EU should establish a standing public–private partnership framework - linked to the proposed European Subsea Cable Governance Authority - to enable regular strategic dialogue between operators, cable manufacturers, repair firms, investors, national administrations, and EU institutions.** The aim is operational: shared risk assessments, coordinated crisis response, and policy development grounded in industry realities rather than regulatory assumptions.

Acknowledgements

The author would like to thank **Chloe Teevan** for their peer review, **Sabine Muscat** for their invaluable input and **Jonathan Hunter** for their constructive feedback. The views expressed in this briefing note are those of the authors and do not necessarily represent those of ECDPM or any other institution. Any errors or omissions remain the responsibility of the authors. For comments and feedback, please contact sap@ecdpm.org.

References

Aldrich, R. and Karatzogianni, A. (2020). Postdigital war beneath the sea? The Stack's underwater cable insecurity. Postdigital Science and Education.

BELLA Programme (n.d.). Building the Europe Link to Latin America: Project Impact and Network Evolution.

Besch, S. and Brown, E. (2024). Securing Europe's Subsea Data Cables. Carnegie Endowment for International Peace.

Braw, E. (2025a). How the Baltic Sea nations have tackled suspicious cable cuts. Atlantic Council.

Braw, E. (2025b). As US tech giants become cable giants, its time we pay attention to out seabeds. Politico.

Burwell, F. and Propp, K. (2026). Digital sovereignty: Europe's declaration of independence? Atlantic Council.

Chen, S. (2025). China unveils a powerful deep-sea cable cutter that could reset the world order. South China Morning Post. (Accessed: 12 March 2026).

Chiappa, C. and Ngendakumana, E. (2023). 'Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says. Politico.

Colasante, L. (2026). The Weaponisation of Infrastructure Starts Underwater.

Dobberstein, L. (2024). Hyperscalers are carving up the ocean floor into private internet highways. The Register. (Accessed 10 March 2026).

Eddy, N. (2025). Subsea Cable Market Expands as AI, Geopolitics Reshape Global Networks. Data Center Knowledge.

EllaLink (2025). About: EllaLink. (Accessed: 12 March 2026).

European Commission (n.d.). Backbone connectivity for Digital Global Gateways. Shaping Europe's Digital Future. (Accessed 10 March 2026).

European Commission (n.d.). Global Gateway. (Accessed 10 March 2026).

European Commission (2024a). The Connecting Europe Facility (CEF Digital).

European Commission (2024b). Commission Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures. Brussels: European Commission.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025). Joint Communication to the European Parliament and the Council: An International Digital Strategy for the European Union (JOIN(2025) 140 final). Brussels: European Commission and High Representative of the Union for Foreign Affairs and Security Policy.

European Commission (2026a). Commission increases submarine cable security with €347 million investment and new toolbox. Press Release. Brussels: European Commission. (Accessed 10 March 2026).

European Commission (2026b). EU Cable Security Toolbox and List of Cable Projects of European Interest (CPEIs). Brussels: European Commission.

European Parliament and the Council of the European Union (2022a). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Brussels: European Union. (Accessed: 12 March 2026).

European Parliament and the Council of the European Union (2022b). Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive). Brussels: European Union. (Accessed: 12 March 2026).

Farrell, H. and Newman, A. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security (2019) 44 (1): 42–79. https://doi.org/10.1162/isec_a_00351.

Federal Communications Commission (2025). Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks. Federal Register: The Daily Journal of the United States Government. (Accessed 10 March 2026).

Folkman, V., Chihaia, M. and Hernandez, I. (2025). Beyond the Action Plan: Towards a Holistic Strategy for a Competitive and Secure Subsea Infrastructure in Europe. European Policy Centre.

GÉANT (2023). GÉANT signs EUR 40 million agreement with the European Commission, the European Investment Bank and AFR-IX Telecom on MEDUSA submarine cable project to boost trans-Mediterranean R&E connectivity. GÉANT: Connect online.

Ghosh, M. (2025). Securing the Unseen Backbone: Strengthening EU Policy for Undersea Communication Cables. North Atlantic Policy Forum.

Google (2020). Announcing the Grace Hopper subsea cable, linking the U.S., U.K. and Spain. Google Cloud. (Accessed 10 March 2026).

Hawkins, N. (2026). Subsea cable investment hits new heights as AI drives demand for ocean bandwidth. Capacity global. (Accessed 10 March 2026).

ISPC (2025). Damage to Submarine Cables from Dragged Anchors. ICPC Viewpoints. (Accessed 10 March 2026).

Lausberg, P. (2026). Can the European Competitiveness Fund deliver? Strengths, shortcomings and recommendations for an effective EU industrial policy. European Policy Centre.

Lipscombe, P. (2025). Telecom Italia approves €700m Sparkle subsea unit sale. Data Center Dynamics.

Medusa Submarine Cable System (n.d.). About us. (Accessed: 12 March 2026).

Meta (2025). Unlocking global AI potential with next-generation subsea infrastructure. Engineering at Meta.

Nokia (2025). Nokia completes its sale of leading submarine networks business, ASN (Alcatel Submarine Networks), to the French State. Espoo/Paris: Nokia Press Office.

Orange (2025). Orange Marine modernizes its fleet of cable ships to secure digital infrastructure in Europe, Africa and the Middle East. Press Release, Orange Newsroom.

Petrova, M. (2025). Underwater cables are a vital piece of the AI buildout and internet — investment is booming. CNBC.

Plucinska, J. (2022). Nord Stream gas 'sabotage' who's being blamed and why?. Reuters.

Submarine Cable Infrastructures Expert Group (2026). Security and Resilience of EU Submarine Cable Infrastructures: Submarine Cable Security Toolbox and Cable Projects of European Interest. Submarine Cable Infrastructures Expert Group.

Submarine Cable Infrastructures Expert Group (2025). Security and Resilience of EU Submarine Cable Infrastructures: Mapping, Risk Assessments, Stress Tests. Submarine Cable Infrastructures Expert Group.

SubTel Forum (2025). Submarine Telecoms Industry Report: 2025-2026 Global Outlook. Sterling, Issue 14, VA: Submarine Telecoms Forum.

Sytas, A. and Kauranen, A. (2023). Three Baltic pipe and cable incidents 'are related', Estonia says. Reuters.

Telin (n.d.). The Rise of Hyperscalers in Subsea Investments. (Accessed 10 March 2026). Telin.

Tocci, N. and Techau, J. (2026). Can Europe Trust the United States Again? Carnegie Endowment for International Peace.

Endnotes

1. This figure refers specifically to telecommunications cable ships dedicated to maintaining and expanding submarine telecommunications infrastructure, and excludes other vessel types such as survey vessels and power cable ships.
2. When compared to global competitors such as Subcom from the United States and Japan's NEC, ASN's market strength is evident, with the former supplying a total of 9 systems, and 73,810 kilometres of cable and the latter, 8 systems and 66,460 kilometres of cable (Subtelforum 2025).
3. The horizontal security framework for critical infrastructure established through the NIS2 and the Critical Entities Resilience (CER) Directive.
4. The expert group is chaired by the European Commission and comprises representatives from Member States'.
5. The 13 priority areas Cable Projects of European Interest (CPEIs) consist of priority areas identified to enhance EU resilience, where private investment alone may not be commercially viable.
6. As of December 2025, €420 million has been committed to finance 51 projects under the first three CEF Digital calls.
7. Between intra-EU and extra-EU mechanisms.

This publication benefits from the structural support by ECDPM's institutional partners: The Netherlands, Austria, Belgium, Denmark, Estonia, Finland, Ireland, and Luxembourg.