EUROPEAN POLICY CENTRE

DISCUSSION PAPER

EUROPE'S POLITICAL ECONOMY PROGRAMME

EUROPE IN THE WORLD PROGRAMME

20 OCTOBER 2025

Beyond the Action Plan: Towards a Holistic Strategy for a Competitive and Secure Subsea Infrastructure in Europe

Varg Folkman
Mihai Sebastian Chihaia
Ian Hernandez

Credit: CANVA

Table of contents

ABOUT THE AUTHORS

Varg Folkman is a Policy Analyst at the European Policy Centre Europe's Political Economy Programme.

Mihai Sebastian Chihaia is a Policy Analyst at the European Policy Centre's Europe in the World Programme.

Ian Hernandez is a Junior Policy Analyst at the European Policy Centre Europe's Political Economy Programme.

ACKNOWLEDGEMENTS / DISCLAIMER

The support the European Policy Centre receives for its ongoing operations, or specifically for its publications, does not constitute an endorsement of their contents, which reflect the views of the authors only. Supporters and partners cannot be held responsible for any use that may be made of the information contained therein.

This Discussion Paper is the result of two dedicated roundtables held in spring 2025, as well as interviews and discussions with policymakers, industry practitioners, and experts. Developed in the framework of the project on the future of EU subsea infrastructure policy, the EPC is grateful for the involvement of its partner, the Vodafone Institute.

Vodafone Institute for Society and Communications

Executive summary

Once an invisible backbone of global connectivity, subsea cables are quickly becoming a strategic concern. As demand for internet services rises, investment in new fibre-optic infrastructure is accelerating – and with it, geopolitical attention. The seabed has emerged as a new frontier of hybrid warfare among Europe, Russia and other actors.

Ownership dynamics in the sector are also shifting. Just four US cloud providers now control 71% of global subsea fibre capacity, overtaking traditional telecom carriers and driving most new projects. Europe lags behind in new seabed infrastructure, as its carriers struggle to keep up with their counterparts across the Atlantic. Although the EU funds strategic projects, its investment is dwarfed by cloud hyperscalers.

Awareness of cable networks' strategic value is growing. Concerns over vendors from unreliable countries in subsea and other critical infrastructure and vulnerabilities to hybrid attacks are prompting the EU and NATO to coordinate more closely. But more needs to be done, particularly in public-private cooperation: Europe's capacity to repair damaged cables is limited, and private repair and maintenance agreements are not scaled to respond to coordinated seabed attacks.

Furthermore, there are few global standards ruling the subsea industry. Few laws cover modern issues like acts of hybrid warfare, and international governing bodies remain private initiatives.

To respond, the EU must follow and go beyond the European Commission's 2024 Action Plan on Submarine Cable Security. A comprehensive strategy should accelerate cross-border mapping and risk assessment. This includes identifying vulnerabilities and strengthening repair and resilience capabilities across jurisdictions.

This paper sets out 10 proposals to advance the EU's Action Plan on Cable Security and strengthen Europe's strategic position. As the seabed becomes a new arena of economic and military rivalry, Europe must act to protect its links, resilience and global edge.

1. Designate subsea cables as services of general economic interest

2. Expand and target EIB funding

3. Coordinate and expand EU funding sources

4. Apply the IPCEI model to cable projects

5. Incentivise consolidation among EU operators

6. Remove barriers hindering international competitiveness

7. Champion the ICPC as a standard-setting body

8. Develop a state-backed insurance model

9. Design a strategic coordination framework that can be used as a best-practice guide at the national level

10. Reinforce EU-NATO coordination and develop an integrated doctrine

Introduction

The network of fibre, power and gas cables crisscrossing the ocean floor has drawn unprecedented attention in recent years. Headline-grabbing reports of cable breakages have helped drive this surge in interest, but a deeper awareness of the vulnerabilities and market dynamics behind the global web connecting Europe's internet and electricity systems is also taking hold. For an industry that long relied on "security through obscurity",[1] such visibility is both a blessing and a curse.

Subsea infrastructure has become geopolitical in every sense – both a target in hybrid warfare by hostile nations and a stage for the transatlantic contest over technological sovereignty. Often called the world's backbone infrastructure, these cables provide vital services with no equivalent alternatives.

Demand for subsea capacity is soaring. The telecoms segment, in particular, is experiencing its highest investment expansion since the dot-com boom of the early 2000s, with $13 billion worth of new fibre-optic cables set to come online between 2025 and 2027.[2] This surge is driven mainly by US cloud providers, often referred to as hyperscalers, and digital content providers seeking even greater data throughput. Subsea cables carry 97-98% of all global internet traffic. Google, Meta, Microsoft and Amazon alone account for 71% of total subsea cable capacity and continue to dominate new cable investments.[3]

Energy infrastructure, though more regional in nature, is also facing a boom of its own. The green transition and efforts to build a single European energy market have sharply increased demand for subsea cables connecting EU electricity markets. Capacity among suppliers is stretched, with energy infrastructure demanding specialised production facilities and vessels for installation.

With foreign companies threatening to supplant EU incumbents, Europe stands to lose market shares, technical capabilities and know-how in the subsea sector to US and Chinese rivals. This trend has far-reaching implications for the Union's competitiveness, security and technological sovereignty.

Most new fibre-cable investments now originate from the US hyperscalers. Moreover, as with 5G infrastructure, Chinese manufacturers are suspected of involvement in EU-based subsea cable networks, though the full extent remains unclear. The growing importance of these networks has heightened concerns that they could be weaponised by hostile governments[4] – or even be leveraged by private actors seeking influence over critical infrastructure.[5]

Europe's capacity to repair and maintain subsea cables in the event of failure or sabotage is limited and uneven across sectors. Energy infrastructure repairs, in particular, face long lead times due to a shortage of specialised vessels and replacement equipment. Being lighter and more standardised, fibre cables are easier to fix, but operators still face bureaucratic obstacles such as national licensing schemes or the need to repair in waters controlled by sanctioned entities.

Overall, the industry suffers from a lack of common standards, both within the EU and globally. No single framework governs how this vital layer of shared infrastructure is managed. Oversight remains fragmented in many countries, with national authorities applying complex and sometimes overlapping rules.

Europe now needs a holistic strategy that considers the full spectrum of issues shaping the subsea ecosystem. Such a strategy should tackle the shifting ownership of subsea infrastructure within and beyond Europe, support sustainable funding models and keep strategic nodes of connectivity in European hands.

Installing cables or launching projects can entail significant financial and logistical hurdles. Depending on length, complexity and cable type, costs can range from hundreds of millions to billions of euros. In Europe, such projects are typically funded through consortia, while US hyperscalers have the financial means to get projects off the ground on their own. EU funding for cable projects is oversubscribed and lacks the strategic foresight needed in the industry.

With its Action Plan on Cable Security, the European Commission has taken an important step toward addressing concerns about the physical protection of subsea networks. Yet the initiative does little to tackle the wider structural and economic challenges facing the EU industry.

Europe now needs a **holistic strategy** that considers the full spectrum of issues shaping the subsea ecosystem. Such a strategy should tackle the shifting ownership of subsea infrastructure within and beyond Europe, support sustainable funding models and keep strategic nodes of connectivity in European hands. It must also extend budding debates about dual-use components and the cybersecurity risks of relying on third countries to the subsea domain. Finally, it must develop a pragmatic approach to protecting existing assets against sabotage.

While there are common challenges across the different types of subsea cables, this report focuses primarily on the telecommunications segment.

Changing market dynamics

The network of seabed fibre cables is expanding rapidly, with at least 650 stand-alone fibre cables connecting countries globally in 2025.[6] In Europe, fibre and power cables span the Baltic, North and Mediterranean Seas, as well as the English Channel. Ireland, Portugal and England serve as the main landing points for transatlantic cables, while France, Greece and Italy play the same role for connections arriving from the East through the Suez Canal.

Europe has long been a central player in the cable industry. Its traditional operators – such as Orange, Telefonica and Vodafone – and its constructors, including Alcatel Submarine Networks (ASN), Nexans, NKT and the newer entrant Prysmian, have shaped the global market. Yet European firms now face challenges from US, Japanese and Chinese rivals. The most significant development has been the entry of the US hyperscalers as funders and operators of fibre cables.

With the explosion of global internet use– a trend that is expected to continue, with some estimates projecting a twentyfold increase in data consumption by 2030 compared with 2020[7] – digital content providers have overtaken telecom operators as the main players in subsea infrastructure.

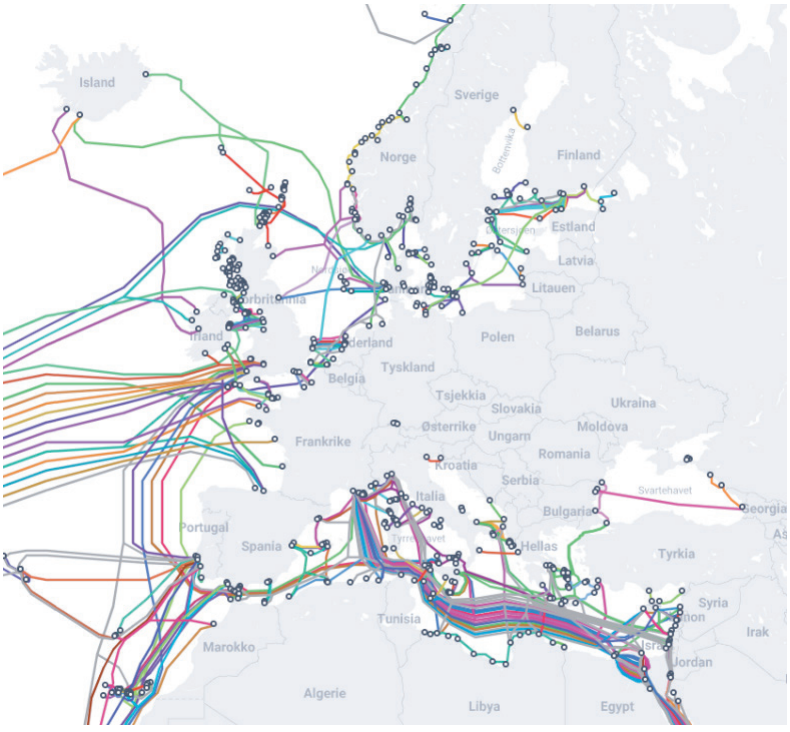
Rather than joining consortia, though they occasionally do, companies like Google and Amazon increasingly opt to construct private cables. With the financial means to fund projects independently, hyperscalers can bypass the lengthy coordination processes of consortia, building cables to their own technical specifications.

While this shift challenges Europe's traditional operators, it has also brought benefits. The entry and gradual dominance of hyperscalers has expanded global connectivity, connected previously underserved regions and improved redundancy in international networks.

This transformation has also sparked fears that European industry is falling behind in cable construction, risking the loss of technological sovereignty. Cables built and operated by companies such as Google are privately owned and largely unregulated, limiting public authorities' influence over their management or the allocation of capacity.[8] Network geography is also shifting under US tech leadership: where cables once linked major population centres, newer cables often connect data centres. With only 1% of telecoms cables under government ownership, direct state control of this critical infrastructure is minimal.[9]

Figure 1

SUBMARINE CABLE MAP



Source: TeleGeography.

The shift in ownership raises wider sovereignty concerns. States can weaponise interdependencies to pursue political goals – but so can corporations. As ownership concentrates in a handful of firms, states can in turn exploit corporate dependencies for strategic ends.[10] US tech giants have previously cooperated with Washington on surveillance demands.[11] Meta, meanwhile, has shown a willingness to cater to China's preferences, casting serious doubt on whether it can be trusted to own and operate Europe's backbone infrastructure.[12]

While the links between the Chinese state and major Chinese constructors such as HMN Tech, once owned by Huawei, are well known, risks of interference extend to the United States as well. The US company SubCom, responsible for several trans-Atlantic cables such as Havfrue 2 connecting the US, Ireland, Norway and Denmark, has well-known ties to American national and military intelligence structures.[13] As transatlantic relations fray, this fact raises serious questions about the wisdom of allowing SubCom to construct vital segments of transatlantic infrastructure.

For the EU, the United Kingdom's strategic position as a digital gateway also requires careful consideration. The majority of transatlantic data traffic lands in the UK before being transmitted to mainland Europe. This necessitates a close and structured partnership with London in any effort to strengthen EU sovereign control over subsea infrastructure.

States can weaponise interdependencies to pursue political goals – but so can corporations. As ownership concentrates in a handful of firms, states can in turn exploit corporate dependencies for strategic ends. US tech giants have previously cooperated with Washington on surveillance demands. Meta, meanwhile, has shown a willingness to cater to China's preferences.

European funding

The EU has begun to take note of its increased reliance on foreign actors in the subsea industry, though the issue still receives far less attention than security and defence. In official documents, increased funding for backbone infrastructure is usually framed as a way to enhance the security and resilience of vital connectivity networks.[14] The focus remains on connecting underserved regions, with support from the Connecting Europe Facility – Digital (CEF Digital) requiring cables to link "one or several of its islands, outermost regions, or overseas countries and territories."[15]

No conditions exist to prioritise funding of EU firms or technologies, although only companies established in a member state or under Union law are eligible to apply.[16] As few cables are built through public procurement, recent calls for "Made in Europe" clauses in EU tenders will have little impact on the industry. By 2027, CEF Digital will have channelled €1 billion into subsea infrastructure, with funding rounds oversubscribed[17] – a significant sum, but modest compared with private investment levels.

The Commission is also preparing a list of Cable Projects of European Interest (CPE), which will receive priority funding and aim to bolster the resilience of EU backbone infrastructure. These projects are intended to serve Europe's strategic objectives in otherwise unbankable projects, though the details on their selection and criteria remain unclear as of writing.[18]

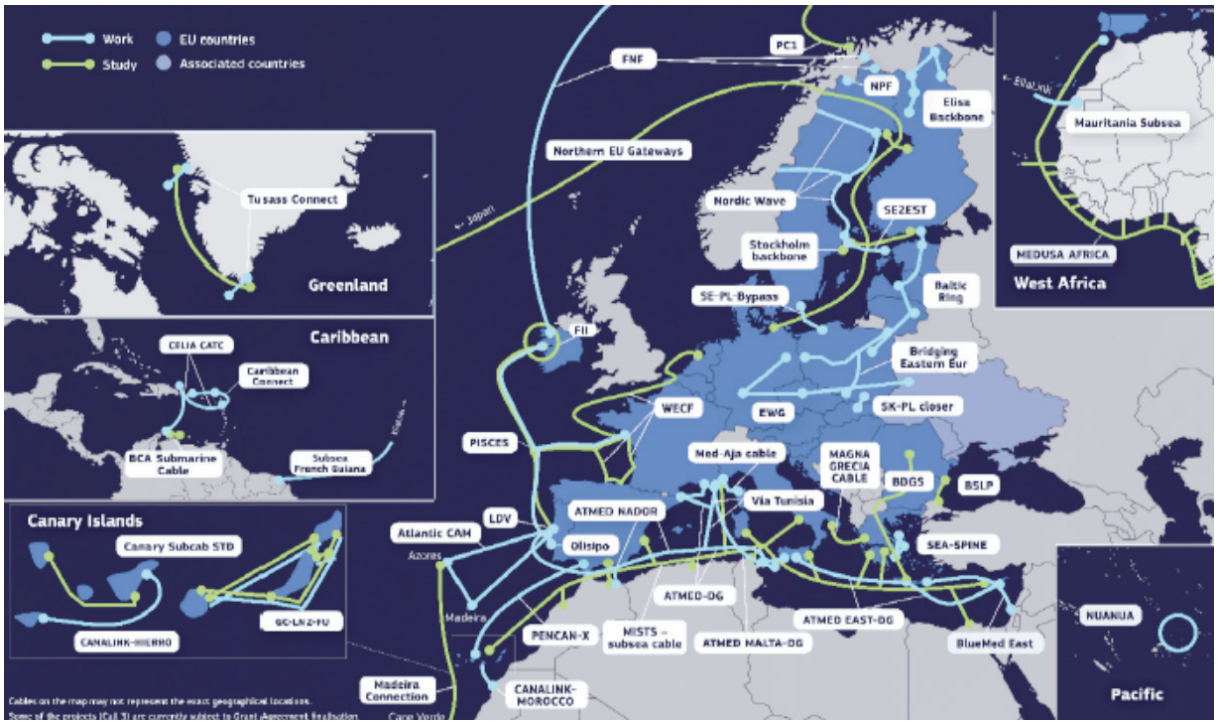
The European Investment Bank (EIB) is likewise active in providing financing support for subsea projects in Europe and connecting it to other regions. The EIB helps the Commission deliver grants under CEF Digital but provides its own financing only as commercial loans for bankable projects. While the bank does not back unprofitable ventures, preliminary EIB approval can help attract additional investors, making a project bankable.

Other funding sources, such as national developmental banks and the Global Gateway initiative, also contribute, but coordination across these instruments remains weak. Funding streams often lack clear strategic prioritisation or conditionalities beyond commercial viability.

To mitigate single points of failure, the EU should create dedicated funding mechanisms under the CEF or similar instruments to support cable redundancy, cross-border connectivity and the modernisation of legacy landing stations.

Figure 2

PROJECTS FUNDED UNDER CEF DIGITAL, ROUNDS 1 TO 3



Source: European Commission.

Unreliable actors

Across EU policy discussions on critical infrastructure, there is a growing recognition of the need to reduce dependence on vendors from unreliable third countries. Cybersecurity threats and fears of export restrictions on key components have already prompted several energy infrastructure projects to exclude or restrict involvement of high-risk countries.

A Baltic offshore wind project, for instance, dropped its Chinese suppliers following pressure from the German *Bundeswehr*.[19] The European Commission has ruled that hydrogen projects sourcing more than 25% of their capacity from Chinese equipment are ineligible for Hydrogen Bank funding, while Lithuania has banned Chinese inverters from its energy grid.[20,21]

Similar debates are unfolding in the US. Under the Clean Network initiative, Washington has sought to curb Chinese participation in subsea cable production – both to projects with landing points in the US and in strategic projects involving American or allied partners internationally.[22] The US has also used its geopolitical leverage to block Chinese involvement in a strategic cable route from France to Singapore, which connects several countries along its path.[23]

In Europe, by contrast, scrutiny of Chinese involvement in subsea infrastructure remains limited. While incidents involving Chinese vessels in cable breakages have sparked outrage, no systematic effort has been taken to map Chinese vendors' participation in cable ownership, construction or component supply. Yet such an initiative has precedent: the EU cybersecurity agency, ENISA, previously mapped Chinese involvement in terrestrial 5G infrastructure.

China's use of export licensing to restrict critical raw materials and technologies, most recently during trade conflicts with the EU and US this spring, puts the risks of dependence in sharp relief. Increasingly, the export license system extends to critical technologies and their components, amplifying Europe's exposure to potential coercion.[24]

Subsea battleground

Subsea infrastructure suffers frequent disruption – about 200 incidents each year, according to the International Cable Protection Committee.[25] While most faults and shunts are caused by natural events such as seismic activity, fishing gear, anchors, or weather phenomena, the number of deliberate attacks has grown. This trend has heightened awareness of the seabed as a new frontier of hybrid warfare.

Recent years have seen a series of high-profile incidents. In 2022, telecom cables to Svalbard cable were disrupted, followed by damage to the Balticconnector gas pipeline and two telecommunications cables between Finland and Estonia in 2023. In 2024, a telecommunications cable linking Sweden and Lithuania was cut, as was another from Finland to Germany. That December, the EstLink power cable and four additional telecommunications lines were damaged.[26]

The scale of the subsea network has grown dramatically over the last decade – from roughly one million kilometres in 2014 to 1,7 million in 2025.[27] This expansion has created a complex tapestry demanding engagement by governments, armed forces, international organisations and private operators.

The nature of threats has also evolved. Incidents now range from service and communications disruptions to hostile actors testing military response capabilities – how many simultaneous cuts can Europe handle? Many intentional incidents employ grey zone tactics: for instance, commercial ships sailing under flags of third countries or linked to ghost companies, making attribution and defence difficult.

Table 1. Timeline of incidents.

2022	Nord Stream pipeline sabotage
2022	Svalbard telecom cables disrupted
2023	Balticconnector gas pipeline and two telecommunications cables damaged
2024	Red Sea cables damaged
2024	Two submarine telecommunication cables, the BCS East-West Interlink and C-Lion1 fibre-optic cables, disrupted in the Baltic Sea
2024	EstLink power cable and four telecommunications cables damaged
September 2025	Multiple cable breaks in the Red Sea

Vulnerabilities are not confined to the seabed. Cable landing stations – where undersea cables connect to terrestrial networks – are often accessible by land and lightly protected. Any strategy to secure Europe's subsea infrastructure must consider these onshore nodes.

EU and NATO responses to grey-zone events

The spate of recent subsea incidents in the Baltic and Nordic Seas has sharpened EU and NATO assessments of grey-zone threats from Russia. The fear is that these disruptions may be test cases – preparing for an increase in attacks on underwater infrastructure and probing allied response speed and capacity.

In response, the EU and NATO have scrambled to coordinate their actions through new joint mechanisms. The EU-NATO Task Force on the Resilience of Critical Infrastructure identified the dangers of simultaneous disruptions to multiple subsea cables and flagged Europe's shortfall in repair capacity. It calls to strengthen maritime situational awareness.[28]

NATO has developed a suite of initiatives to address these gaps. It established the Critical Undersea Infrastructure Coordination Cell in 2023 to connect military, civilian and industry stakeholders.[29] This was followed in 2024 by the creation of the Critical Undersea Infrastructure Network and set up the NATO Maritime Centre for the Security of Critical Undersea Infrastructure, within the alliance's Maritime Command (MARCOM). These initiatives focus on public-private cooperation in monitoring and information sharing.[30] In early 2025, NATO launched Operation Baltic Sentry, which deploys patrol aircraft, warships and unmanned platforms to increase surveillance of ships and critical underwater infrastructure in the Baltic Sea.

Together, these measures reflect a strategy built on presence, monitoring, information-sharing and public-private cooperation.[31] The response is also centred around the strategy of "denying deniability", improving attribution and accountability for perpetrators of hostile acts.[32] Attribution remains a core challenge in grey-zone warfare, where state actors often disguise their responsibility behind commercial or civilian fronts.

At the EU level, cable protection has been integrated into the EU Maritime Security Strategy of 2023. The Commission's Recommendation on the Security and Resilience of Submarine Cable Infrastructures in 2024

promotes synergies among member states to enhance the security and resilience of submarine cable infrastructures. The October 2024 "Niinistö report" similarly identifies cable protection as a cornerstone of European resilience and preparedness.[33]

Attribution remains a core challenge in grey-zone warfare, where state actors often disguise their responsibility behind commercial or civilian fronts.

A voluntary, secure incident reporting mechanism should be established, interoperable across sectors and supported by regular joint exercises involving national authorities and private operators. Such a system would strengthen situational awareness, expedite crisis response and deepen trust between public and private stakeholders.

The Commission's 2025 Action Plan on Cable Security builds on these efforts, urging faster implementation of agreed measures and greater voluntary integration of surveillance and intelligence sharing. Structured around four pillars – prevention, detection, response and repair and deterrence – the plan highlights the importance of basin surveillance, enhanced repair capacity and stronger information exchange between the Union, member states, partners and industry. It also proposes advancing "EU cable diplomacy" to protect Europe's global connectivity interests.[34]

Complementary initiatives are emerging in other maritime theatres. The recent EU Black Sea Strategic Approach links various EU initiatives (including the Action Plan) and proposes a regional maritime security hub to coordinate situational awareness, real-time monitoring "from space to seabed," and early-warning systems for potential threats.[35] However, the implementation details remain unclear.

Finally, the EU Ocean Pact (summer 2025) proposes deploying a pilot fleet of unmanned drones to monitor maritime activities and developments to increase the EU's maritime awareness capabilities. It also emphasises strengthening cooperation with partners in the Middle East and North Africa, further embedding subsea infrastructure protection within Europe's broader maritime security architecture.[36]

Lessons learned in cable protection

Recent incidents in the Baltic, North and Red Seas have offered valuable lessons and exposed common challenges in protecting the European seabed from grey-zone activity.

Although EU-NATO initiatives mark real progress, information sharing between industry and government authorities is often hindered by limited trust and commercial competition. Responsibility for subsea cables is distributed across a web of industry operators, national authorities and international institutions – making seamless information sharing vital but difficult to achieve.

Deterring attacks on critical underwater infrastructure is a demanding task, and detecting malign activity requires significant capacity. The Baltic Sea is a well-mapped and relatively small body of water; other bodies, such as the Black Sea, pose greater challenges and will require more resources, including naval assets and patrols, constant monitoring and further coordination between the EU and NATO.

Speed and clarity of attribution are also central to deterrence. Naval forces can gather and analyse data to determine intent and the assets involved, but formally attributing responsibility remains a political decision. Rapid attribution expands the range of possible responses and signals resolve.

Baltic Sentry has also shown that integrating unmanned systems with conventional naval assets is an efficient way to cover wider maritime areas, reduce costs and enhance monitoring of undersea infrastructure.[37] New technologies such as smart cables and quantum sensing can further improve detection speed and accuracy. Member states should prioritise these emerging capabilities and allocate sufficient resources to strengthen maritime resilience.

Repairing the damage

Both subsea energy and fibre infrastructure face persistent challenges in maintenance and repair, though for different reasons. Power cables are large in scale and weight, with components tailored to specific projects. As a result, repair vessels and materials are highly specialised and in short supply. Spare parts are rarely

available on demand; their size and specificity mean they are often manufactured when failure occurs. Some companies now maintain limited stockpiles of parts, but they remain exceptions. For the energy cable sector, the principal constraint is time – especially delays in mobilising ships and sourcing equipment for repairs.

Fibre cables, by contrast, are smaller and less specialised. The current fleet of ships available for repairs and maintenance is limited but broadly adequate for current demands. This balance would collapse, however, if multiple cables were disrupted simultaneously by a malicious actor. Most operators participate in regional repair and maintenance coalitions, which allow them to share resources and avoid keeping their own dedicated repair capacity on hand.

The EU has identified the shortage of vessels as a potential bottleneck in the event of crisis and is considering contracts with existing operators, as well as a medium-term plan to create a multi-purpose EU Cable Vessels Reserve Fleet.[38] Beyond limited numbers, many vessels are ageing and require replacement. Compounding the problem, the sector faces a shortage of skilled labour for cable repair and maintenance.[39]

Apart from capacity issues, repair and maintenance vessels suffer from delays due to onerous licensing regimes when entering territorial waters to perform such services. Under the United Nations Convention on the Law of the Sea (UNCLOS), states have discretion to regulate activities in their territorial waters and, to some extent, in exclusive economic zones. Obtaining the necessary license to operate in territorial waters, particularly for fibre cable repairs, can take weeks, requiring operators to liaise with multiple agencies and authorities.

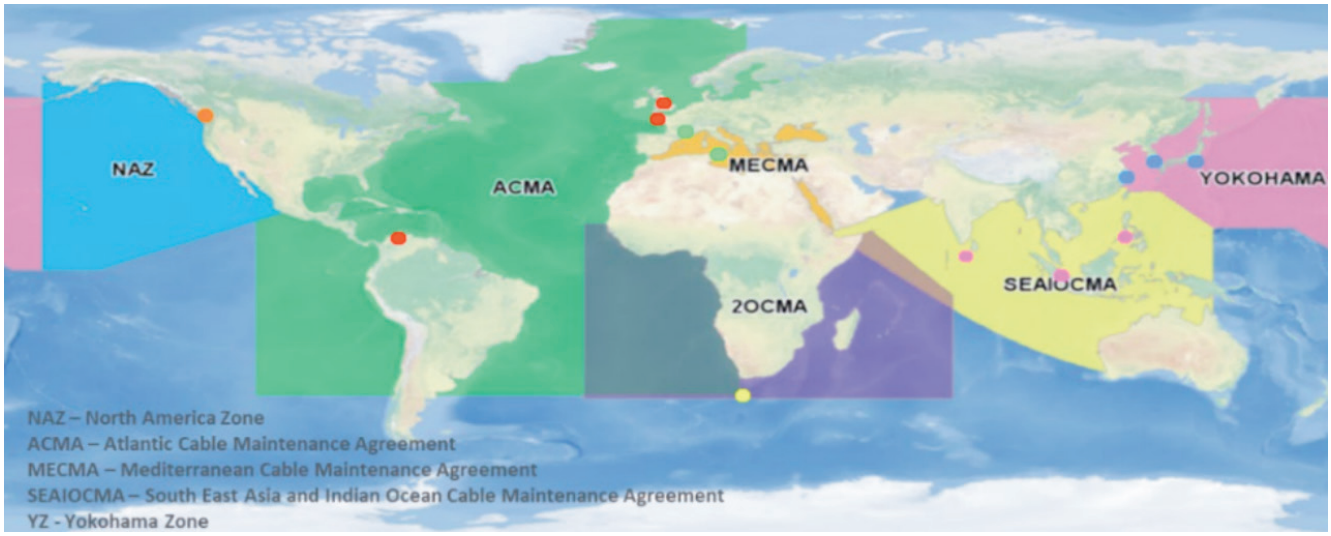
Single points of contact can expedite and simplify procedures but are no guarantee of efficiency; where such offices exist, they are often new and lack institutional memory or established routines. On this issue, US hyperscalers and EU operators share common ground: both call for clearer, faster authorisation processes for repair work in national waters.[40]

The current fleet of ships available for repairs and maintenance is limited but broadly adequate for current demands. This balance would collapse, however, if multiple cables were disrupted simultaneously by a malicious actor.

A further challenge for owners concerns insurance and reinsurance of their assets. Traditional policies exclude acts of war, and insurers have tightened coverage amid rising geopolitical risks. This leaves operators facing higher insurance premiums for specialised war insurance – or lengthy court battles to recover costs.[41]

Figure 3

CABLE MAINTENANCE ZONES



Source: GMSL.

Global standards

This hints at a broader challenge for the subsea sector: a lack of comprehensive global standards governing the industry. The United Nations Convention on the Law of the Sea (UNCLOS) provides the only international legal framework of relevance. It guarantees the freedom to construct cables in international and territorial waters while affirming coastal states' right to impose their own conditions and regulatory frameworks.

A harmonised, lifecycle-based approach to cable security developed jointly with national security, defence and industry partners should underpin all future efforts. End-to-end security guidance and best practices should be formalised and shared, building on the NIS2 Directive on cybersecurity and CER Directive on non-cyber physical resilience of critical entities.

The EU has so far refrained from imposing binding measures on member states for subsea infrastructure. Its Recommendation on Secure and Resilient Submarine Cable Infrastructures remains voluntary, governing mainly security issues relating to cables and complementing the NIS2 and CER Directives.

At the industry level, the International Cable Protection Committee (ICPC) is the leading international forum for subsea cable constructors and operators. Its membership is largely composed of private companies, alongside a handful of national authorities. The ICPC provides non-binding recommendations, mainly on security, but lacks regulatory authority.[42]

Significant regulatory gaps therefore remain, both in Europe and globally. Subsea cables, in particular fibre networks, straddle multiple jurisdictions and regulatory regimes. A holistic set of standards in Europe would be beneficial but would only go so far. While a single set of global standards may be unrealistic in a fraught geopolitical climate, Europe should nonetheless lead regional efforts to align rules and promote consistency across cable governance, including permitting, security protocols and repair coordination.

While a single set of global standards may be unrealistic in a fraught geopolitical climate, Europe should nonetheless lead regional efforts to align rules and promote consistency across cable governance, including permitting, security protocols and repair coordination.

European leadership is equally important to prevent regulatory fragmentation that disadvantages EU operators. For instance, from 2027, EU cable-laying and maintenance ships will be fall under the EU Emissions Trading System (ETS), whereas ships operating from ports outside of the Union, such as in the UK, will not, even if they make repairs or construct cables in EU waters. As some EU operators have noted, this asymmetry could drive operations offshore.

Towards a holistic EU strategy for subsea infrastructure

The importance of subsea cables demands a coordinated European response. Private sector investment has surged, but Europe must match it with sovereign capabilities and policy leadership.

The EU's Action Plan on Submarine Cable Security offers an important starting point – mapping vulnerabilities, assessing risks, and developing a shared toolbox. Building on this, the EU should consider establishing a dedicated EU resilience fund, coordinating governance standards and enhancing civil-military collaboration. Strengthening Europe's repair capacity and securing legacy infrastructure are essential to counter hybrid threats and ensure continuity of service.

The EU should consider establishing a dedicated EU resilience fund, coordinating governance standards and enhancing civil-military collaboration. Strengthening Europe's repair capacity and securing legacy infrastructure are essential to counter hybrid threats and ensure continuity of service.

A harmonised EU–UK–NATO approach is equally vital to guarantee subsea cable resilience across jurisdictions. Consistent application of security protocols, investment oversight and operational coordination will be key to protecting the sinews of Europe's digital and energy connectivity.

The Action Plan is a good step forward but falls short of the comprehensive strategy the sector needs to ensure Europe's long-term competitiveness. It does not yet address the growing debate on third-country access to critical infrastructure, nor does it fully engage with the wider question of Europe's technological sovereignty.

While providing a blueprint for such a holistic strategy falls beyond the scope of this report, we draft 10 proposals that can help tackle some of the issues facing EU industry and the Union as a whole – forming the first building blocks for a truly holistic approach.

1. Designate subsea cables as services of general economic interest

Subsea infrastructure underpins nearly all modern economic and social activity. Fibre cables should therefore be recognised and regulated as services of general economic interest (SGEI). Such a designation would give the EU and its member states greater authority over how capacity is used what conditions apply to cables landings on EU territory and how the infrastructure is governed.

While the EU can already impose conditionalities, such as reservation capacity for public goods to cable projects receiving EU grants, hyperscaler-led cables typically do not involve EU funding and thus fall outside these rules.

Recognising subsea infrastructure as a European Public Good (EPG) would also ease access to public funding for strategic projects. EPGs, defined as initiatives whose value is greater when delivered at EU rather than national level,[43] could cover both intra-EU resilience projects and external connections critical to competitiveness.[44]

2. Expand and target EIB funding

The EIB remains underused as a vehicle for funding subsea infrastructure. Resource constraints have so far limited its role. The EIB should assign dedicated manpower to develop and secure financing for EU-led initiatives. While the bank is confined to commercially viable ventures, it can use its **signalling power**, publicly expressing its intent to invest, to attract external funding. This can help projects reach viability more quickly.

3. Coordinate and expand EU funding sources

The EU already has several instruments that directly or indirectly support subsea cable development, such as the Connecting Europe Facility – Digital (CEF), Global Gateway and the oversight of member state-aid expenditure. These funding streams are fragmented, shaped by differing institutional logics and priorities. The forthcoming Competitiveness Fund could add further opportunities but also risks duplication.

A **Working Group on Strategic Investments in Subsea Infrastructure** should be created to coordinate these sources and align conditionalities and EU funding parameters. Such a platform would enable a more coordinated approach to identifying priority routes to invest in. Currently, the EU lags behind in constructing international routes connecting regions and continents.

It could also explore the establishment of a dedicated **EU Cable Resilience Fund**. This would enable the Union to co-finance and construct strategic cross-continental cables itself, strengthening is resilience and technological sovereignty.

4. Apply the IPCEI model to cable projects

The Commission plans to identify Cable Projects of European Interest (CPEIs) to channel funding under the CEF. Instead of simply listing eligible projects, it should consider applying the **Important Projects of Common European Interest (IPCEI) framework** to the subsea cable sector.

The IPCEI tool enables broad approval of state aid for cross-border industrial initiatives within the Union, fostering cooperation across important value chains. While the current IPCEI has limitations, its framework could be used to attract both public and private financing to cable projects of high importance.[45]

5. Incentivise consolidation among EU operators

Traditional subsea cable operators are losing ground to US hyperscalers largely because they lack funding for capital-intensive projects like new cables. Industry actors attribute this weakness to a fragmented European market, constrained by strict EU merger and acquisition rules. The EU should consider Mario Draghi's proposal **to define telecoms markets at the European rather than national level** to enable strategic consolidation that could unlock investment.[46] However, any relaxation of competition policy must be tied to strong investment commitments by industry players.

6. Remove barriers hindering international competitiveness

Several existing and upcoming regulatory barriers risk undermining the competitiveness of the EU subsea cable sector relative to non-EU rivals. The ETS is a prime example. **Extending ETS coverage to foreign ships operating in EU waters** would correct the loss in competitiveness to rivals not covered by the EU rules. Beyond this, the EU should systematically map and address regulatory obstacles as part of its broader simplification agenda to maintain a level playing field for European operators.

7. Champion the ICPC as a standard-setting body

While no institution currently sets binding global standards for the subsea infrastructure sector, the ICPC already convenes many market actors and several states. The EU should expand the Committee to include more states and encompass an even broader cross-section of the subsea sector.

The ICPC should **strike broad, voluntary and non-binding standards** for the industry. Such norms would lay the groundwork for a future international framework once conditions become more amenable to binding regulation.

8. Develop a state-backed insurance model

Insuring subsea assets has become increasingly difficult. The EU should develop guidelines for a **state-backed insurance and reinsurance mechanism** to bridge the gap between war and non-war coverage.

9. Design a strategic coordination framework that can be used as a best-practice guide at the national level

Member states face persistent gaps in protection responsibilities and in coordinating between national stakeholders, such as defence authorities, regulators and infrastructure operators. The EU should create a **strategic coordination framework** to serve as a best-practice reference at a national level. This guide would outline mechanisms for cooperation across industry, academia and government, drawing on successful models already in place in several member states.

10. Reinforce EU-NATO coordination and develop an integrated doctrine

An integrated EU-NATO conceptual doctrine for undersea infrastructure security and resilience would strengthen public-private coordination, build trust and improve information sharing among institutions, companies and member states. It would also support crisis response, legislative alignment and the integration of lessons learned from prior incidents.

A **trilateral Cable Resilience Coordination Group** should align risk assessments, incident response and investment planning across the EU, UK and NATO via NATO's Critical Undersea Infrastructure Coordination Cell. This unified approach would ensure consistent application of security protocols and investment oversight across jurisdictions.

[1] Starosielski, Nicole (2015), *The Undersea Network*, Durham: Duke University Press.

[2] Brodsky, Paul, "Building Tomorrow's Internet: A 2025 Update on Cable Investment", *TeleGeography*, (Accessed June 15, 2025).

[3] Kang, Jocelinn & Jacob, Jessie (2024), "Connecting the Indo-Pacific", Canberra: Australian Strategic Policy Institute.

[4] Farrell, Henry & Newman, Abraham (2023), *Underground Empire: How America Weaponized the World Economy*, New York: Henry Holt and Co.

[5] Gjesvik, Lars (2022), "Private infrastructure in weaponized interdependence", *Review of International Political Economy*, Volume 30, Issue 2, pp. 722-746.

[6] Burdette, Lane, "How Many Submarine Cables Are There, Anyway?", *TeleGeography* (Accessed June 27, 2025).

[7] Grijpink, Ferry et al. (2020) "Connected world: An evolution in connectivity beyond the 5G revolution", *McKinsey*.

[8] European Commission (2024), "How to master Europe's digital infrastructure needs?" COM (2024), 81.

[9] Nie, Michille, "Meta's Foray Into Undersea Cables Raises Questions Over Critical Infrastructure", *Open Markets Institute* (Accessed June 28, 2025).

[10] Gjesvik (2022).

[11] Farrell & Newman (2023).

[12] Wynn-Williams, Sarah (2025), *Careless People: A story of where I used to work*, London: Pan Books Ltd.

[13] Brock, Joe, "Inside the subsea cable firm secretly helping America take on China", *Reuters* (Accessed June 18, 2025).

[14] European Commission (2024), "Commission Recomendation on Secure and Resilient Submarine Cable Infrastructures" (2024), 1181.

[15] European Commission (2024), "Commission Implementing Decision on the financing of the Connecting Europe Facility – Digital sector and the adoption of the multiannual work programme for 2024-2027", C(2024), 6891.

[16] European Parliament & European Council (2021), "Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations".

[17] European Commission (2025), "EU Action Plan on Cable Security" JOIN (2025), 9.

[18] Ibid.

[19] Jack, Victor, "China could blackmail Germany via wind turbines, report warns", *Politico* (Accessed June 3, 2025).

[20] Dokso, Anela, "EU Excludes Chinese Hydrogen Equipment from Subsidies", *Energy News* (Accessed June 18, 2025).

[21] Norman, Will, "Lithuania to block Chinese inverters with cybersecurity legislation", *PVTECH* (Accessed June 18, 2025).

[22] *U.S. Department of State*, "The Clean Network" (Accessed June 22, 2025).

[23] Brock, Joe, "U.S. and China wage war beneath the waves – over internet cables", *Reuters* (Accessed June 10, 2025).

[24] Wübbeke, Jost & Catarata, Martin (2025), "Chokepoint Politics: China's Export Controls in the Era of Great Power Rivalry", Berlin: Sinolytics.

[25] *International Cable Protection Committee*, "Media Enquiries & Frequently Asked Questions", (Accessed September 18, 2025).

[26] Van Soest, Henri et al. (2025), "Evolving threats to critical undersea infrastructure: Implications for European security and resilience", Santa Monica: RAND

[27] *International Cable Protection Committee*, "Media Enquiries & Frequently Asked Questions" (Accessed September 18, 2025).

[28] European Commission (2023), "EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure".

[29] NATO, "NATO stands up undersea infrastructure coordination cell" (Accessed August 18, 2025).

[30] Allied Maritime Command, "NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure", (Accessed August 18, 2025).

[31] SHAPE, "Baltic Sentry to enhance NATO's presence in the Baltic Sea" (Accessed August 18, 2025).

[32] Allied Maritime Command, "NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure", (Accessed August 18, 2025).

[33] Niinistö, Sauli (2024), "Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness".

[34] European Commission (2025).

[35] European Commission (2025b), "The European Union's strategic approach to the Black Sea region" JOIN(2025), 135.

[36] European Commission, "The European Ocean Pact" (Accessed August 18, 2025).

[37] Naval News Staff, "NATO ACT deploys unmanned vehicles for surveillance in the Baltic Sea", *Naval News* (Accessed August 18, 2025).

[38] Ibid.

[39] UK Parliament Joint Committee on National Security Strategy, "Is the UK prepared for attacks on undersea internet cables? MPs and Lords hear evidence from security experts" (Accessed September 17, 2025).

[40] Næss-Schmidt, Helge Sigurd et al. (2021), "The Economic Impact of the Forthcoming Equiano Subsea Cable in Portugal", *Copenhagen Economics*.

[41] Braw, Elisabeth, "What Is War? Ask an Underwriter", *Foreign Policy* (Accessed September 22, 2025).

[42] Ganz, Abra et. al. (2024), "Submarine Cables and the Risks to Digital Sovereignty", *Minds and Machines*, Volume 34, No. 3.

[43] Fuest, Clemens, Pisani-Ferry, Jean (2019), "A Primer on Developing European Public Goods", *EconPol Policy Report*, No. 16, Munich: Ifo Institute – Leibniz Institute for Economic Research at the University of Munich.

[44] Lausberg, Philipp & Riekeles, Georg (2025), "From mission polity to mission economy: Making the EU a strategic investment power" Brussels: European Policy Centre.

[45] Lausberg, Philipp, Folkman, Varg & Allen, Chris (2025), "Making IPCEIs a new vanguard for EU industrial policy", Brussels: European Policy Centre.

[46] Draghi, Mario (2024), "The Future of European Competitiveness: Part B."

NOTES

The **European Policy Centre** is an independent, not-for-profit think tank dedicated to fostering European integration through analysis and debate, supporting and challenging European decison-makers at all levels to make informed decisions based on sound evidence and analysis, and providing a platform for engaging partners, stakeholders and citizens in EU policymaking and in the debate about the future of Europe.

The EPC's **Europe's Political Economy Programme** (EPE) focuses on EU economic governance, the single market, and digital, industrial, energy, trade, and economic security policies amid significant geo-economic and technological shifts. In a world of rising geopolitical competition and a fragmenting economy, the EPE has been at the forefront of research on Europe's competitiveness agenda, the "triple" green, digital and economic security transitions and 'wartime economy'. The EPE's cross-programme flagship initiative, the Brussels Economic Security Forum, examines EU-US-China dynamics, changing international economic rules and statecraft, as well as related EU policy challenges. As fast advancing components of economic security, critical emerging technologies in clean tech, the AI value chain and quantum are priority areas of focus. Using its convening power and multistakeholder taskforce model, the Programme aims to provide in-depth analysis and actionable recommendations to tackle key policy challenges. The EPE team comprises a diverse group of analysts with backgrounds from government, the private sector, academia, and journalism, bringing a broad range of expertise to its work.

The **Europe in the World** (EiW) **Programme** scrutinises the impact of a changing international system on Europe and probes how the EU and its member states can advance their interests and values on a regional and global level. It examines the EU's relations with both major and middle powers around the world, and how Europe can continue to contribute to a rules-based global order. Secondly, the Programme focuses on the role of the EU in fostering reform, resilience and stability in neighbouring regions and looks closely at developments in Turkey and Ukraine, among other countries. Thirdly, the Programme examines and seeks to advance the development of Europe's security and defence policy.

With the strategic support of King Baudouin Foundation
Working together for a better society

Co-funded by the European Union