Report by the Expert Group under Recommendation 2024/779
on Secure and Resilient Submarine Cable Infrastructures

Security and Resilience of EU Submarine Cable Infrastructures

Mapping, Risk Assessments, Stress Tests

Annex

October 2025

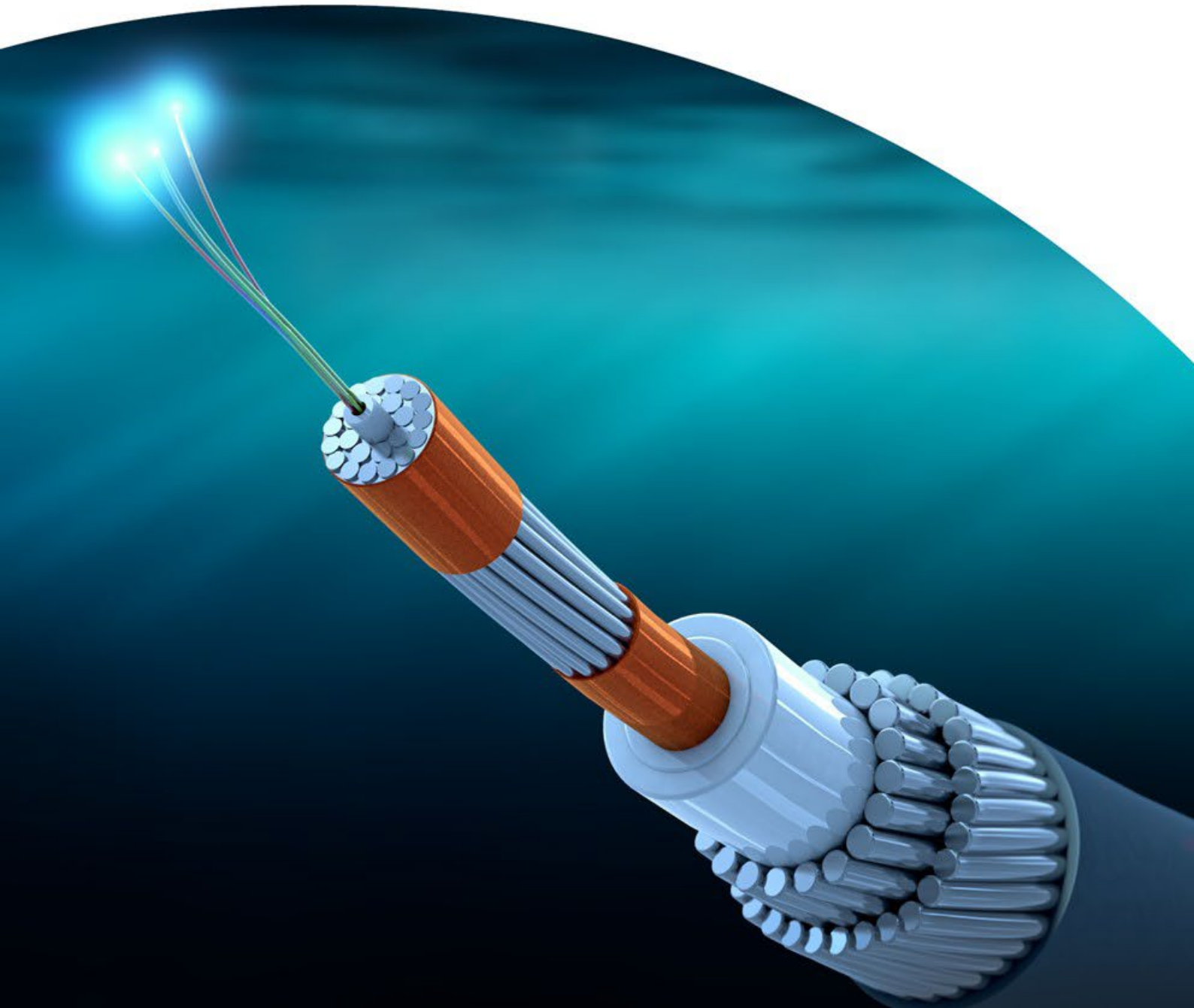


Table of Contents

1. INTRODUCTION

This report constitutes an annex to the Expert Group's report on 'Security and Resilience of EU Submarine Cable Infrastructures: Mapping, Risk Assessments, Stress tests'. It contains detailed factual information that complements the content of the main body of the report.

The methodological framework used in this report is aligned with the requirements set out in Recommendation (EU) 2024/779. ([1]) The Recommendation emphasises the critical need to implement robust measures to enhance the security and resilience of submarine cable infrastructures across Europe. This annex is structured in a way that follows the requirements set out in the Recommendation:

- **Section 2: Legal and administrative framework** provides an overview of the legal and administrative framework for submarine cables, considering the United Nations Convention on the Law of the Sea (UNCLOS), the EU maritime security framework, the EU framework for critical entities resilience and cybersecurity framework, as well as a desktop review of relevant papers and announcements to provide the wider policy context. Information in this section builds on feedback from Member States provided through the Expert Group and information from the contractor supporting the Expert Group.
- **Section 3: The submarine cable market and ecosystem** provides an overview of the submarine cable market, value chain and ecosystem, including key stakeholders, the installation, maintenance and repair procedures, as well as an analysis of the vessel fleet and funding models. Information in this section comes from the contractor supporting the Expert Group.
- **Section 4 Mapping of cable infrastructures in the EU** maps and presents a capacity analysis of submarine cables landing in EU Member States, along with a review of the faults affecting these cables over time. It also describes the associated land-based infrastructure, data centres, cloud regions and internet exchange points (IXPs). The analysis presented in this section was created using a mapping tool specifically developed for this report (not public), which is based on Analysys Mason's submarine cable database, ([2]) Axiom's expertise and public announcements from submarine cable owners. This information has been validated through comparison with other third-party sources, such as the Submarine Telecoms Forum Almanac, ([3]) the ITU-T BB map, ([4]) Infrapedia ([5]) and TeleGeography. ([6]) It fulfils the requirements set out in Point 16 of Recommendation (EU) 2024/779, in conjunction with Points 5 and 6, as well as Recitals 18, 19 and 24, which require the mapping of existing submarine cable infrastructures at the EU level.

([1]) European Commission (2024), *Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures*.

([2]) Analysys Mason (2025), *Submarine cable database 1H 2025*.

([3]) Submarine Telecoms Forum (2025), *Submarine cable Almanac*.

([4]) ITU (2025), *Infrastructure Connectivity Map*.

([5]) Infrapedia (2025), *The world's largest network and datacenter infrastructure atlas*.

([6]) TeleGeography (2025), *Submarine Cable Map*.

2. LEGAL AND ADMINISTRATIVE FRAMEWORK

Legislation and policy frameworks governing submarine cables span a range of areas, some of which are specifically focused on submarine cables, while others address broader issues that are indirectly relevant to submarine cables. This section provides an overview of applicable frameworks and legislation under UNCLOS, relevant EU policies, guidance issued by the North Atlantic Treaty Organization (NATO) and Member State regulations.

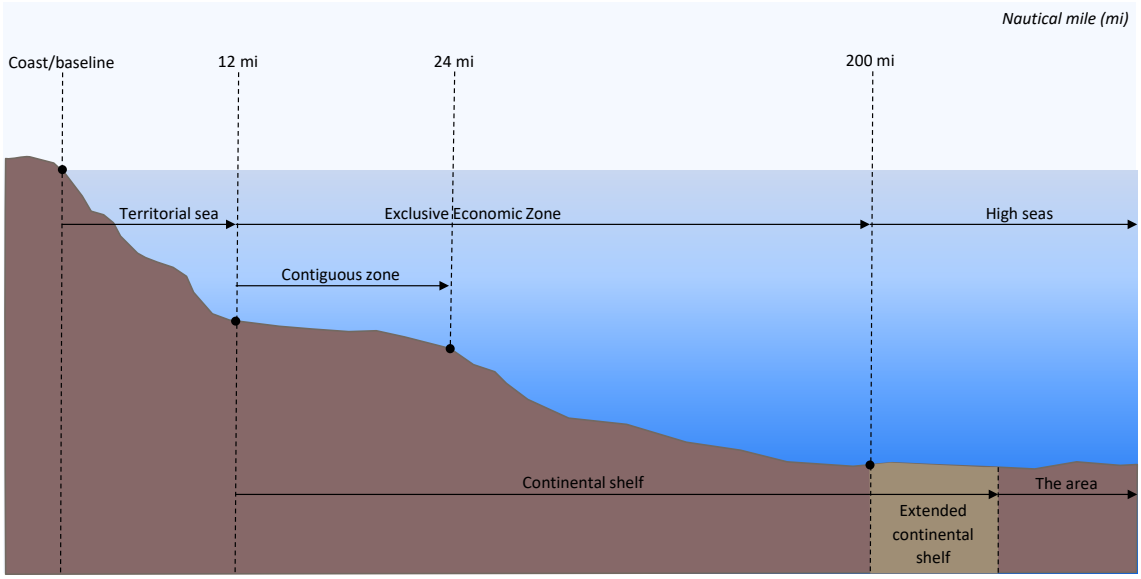
2.1. The United Nations Convention on the Law of the Sea

The United Nations Convention on the Law of the Sea (UNCLOS), which was adopted on 10 December 1982 and entered into force on 16 November 1994, lays down a comprehensive regime of law and order in the world's oceans and seas, establishing rules that govern all uses of the oceans and their resources.

2.1.1. Maritime zones and boundaries

UNCLOS defines the maritime zones recognised under international law, which determines the legal jurisdiction of each coastal State; these zones are illustrated in Figure 2.1.

Figure 2.1: Maritime zones and boundaries [Source: Analysys Mason, 2025]



- **The territorial sea** extends "up to a limit not exceeding 12 nautical miles, measured from baselines determined in accordance with this (UNCLOS) Convention". It is an area over which the "sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea". UNCLOS includes provisions for complex coastlines, stating that "in localities where the coastline is deeply indented and cut into, or if there is a fringe of islands along the coast in its immediate vicinity, the method of straight baselines joining appropriate points may be employed in drawing the baseline from which the breadth of the territorial sea is measured". ([7])

([7]) United Nations (1982), *United Nations Convention on the Law of the Sea*, Articles 2, 3 and 7.

- The **contiguous zone** "may not extend beyond 24 nautical miles from the baselines from which the breadth of the territorial sea is measured". Within this zone, the coastal State "may exercise the control necessary to prevent infringement of its customs, fiscal, immigration or sanitary laws and regulations within its territory or territorial sea" and "punish infringement of the above laws and regulations committed within its territory or territorial sea". ([8])

- **The Exclusive Economic Zone (EEZ)** extends up to a distance of 200 nautical miles (approximately 370.4 km) from the baselines from which the breadth of the territorial sea is measured. The coastal State has "sovereign rights for the purpose of exploring and exploiting, conserving and managing the natural resources, whether living or non-living, of the waters superjacent to the seabed and of the seabed and its subsoil and with regard to other activities for the economic exploitation and exploration of the zone, such as the production of energy from the water, currents and winds". The coastal State has also jurisdiction as provided for in the Convention in relation to the establishment and use of artificial islands, installations and structures, marine scientific research, the protection and preservation of the marine environment, and other rights and duties provided for in the Convention". ([9])

- **The high seas** are "all parts of the sea that are not included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelagic State". According to Article 87 (1) of UNCLOS, "the high seas are open to all States, whether coastal or land-locked. Freedom of the high seas is exercised under the conditions laid down by this Convention and by other rules of international law. It comprises, *inter alia*, both for coastal and land-locked States: a) freedom of navigation, b) freedom of overflight, c) freedom to lay submarine cables and pipelines, subject to Part V1, d) freedom to construct artificial islands and other installations permitted under international law, subject to Part VI, e) freedom of fishing, subject to the conditions laid down in Section 2, f) freedom of scientific research, subject to Parts VI and XIII ". No State may validly purport to subject any part of the high seas to its sovereignty. Every State, whether coastal or land-locked, has the right to sail ships flying its flag on the high seas". ([10])

Under Article 21 of UNCLOS, coastal States may, but are not obligated to, adopt necessary laws and regulations, in conformity with UNCLOS and other rules of international law, to protect submarine cables within their territorial waters. UNCLOS also provides coastal States with law-enforcement duties and obligations in the contiguous zone, such as regulations related to immigration, but it does not grant jurisdiction over submarine cables in this zone.

Articles 79, 87 and 112 to 115 of UNCLOS contain specific provisions that govern the laying, maintenance and protection of submarine cables in maritime zones beyond the territorial sea:

- Article 79(2) states that "subject to its right to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources and the prevention, reduction and control of pollution from pipelines, the coastal State may not impede the laying or maintenance of such cables or pipelines."

- Article 79(3) clarifies that "the delineation of the course for the laying of such pipelines on the continental shelf is subject to the consent of the coastal State."

([8]) *Ibid*, Article 33.

([9]) *Ibid*, Articles 55, 56 and 57.

([10]) *Ibid,* Articles 86, 87, 89 and 90.

- Article 87(1c) grants to all States, the "freedom to lay submarine cables and pipelines" in the high seas, subject to Part VI (of UNCLOS)."
- Article 112 stipulates that "all States are entitled to lay submarine cables and pipelines on the bed of the high seas beyond the continental shelf."
- Article 113 mentions that States must adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence, is a punishable offence.. This is discussed further in Section 2.1.2.
- Articles 114 establishes that "every State shall adopt the laws and regulations necessary to provide that, if persons subject to its jurisdiction who are the owners of a submarine cable or pipeline beneath the high seas, in laying or repairing that cable or pipeline, cause a break in or injury to another cable or pipeline, they shall bear the cost of the repairs."
- Article 115 requires "every State to adopt the laws and regulations necessary to ensure that the owners of ships who can prove that they have sacrificed an anchor, a net or any other fishing gear, in order to avoid injuring a submarine cable or pipeline, shall be indemnified by the owner of the cable or pipeline, provided that the owner of the ship has taken all reasonable precautionary measures beforehand."

2.1.2. Legal measures penalising damage-causing vessels

Article 113 of UNCLOS establishes, among other provisions, that "every state shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas, done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence". With respect to this provision, it should be noted that:

- Some States Parties to UNCLOS are also Parties to the 1884 International Convention for the Protection of Submarine Telegraph Cables. While many of the 1884 Convention's obligations have been integrated into UNCLOS, not all of the provisions have been incorporated.
- Fines for cable damage provided for in some national legislations do not always serve as an effective deterrent against such actions.

As an example, in May 2024, the Cook Islands enacted new legislation that imposes fines of up to EUR 135 000 on those entities that negligently damage submarine cables. Other sanctions include mandatory reporting of such incidents, with fines of up to EUR 10 000, approaching the best international standards adopted by Australia, New Zealand and Uruguay in this area to create a deterrent effect against negligent actors. In early 2024, Panama also approved a resolution by the Panama Maritime Authority that includes sanctions of up to EUR 9000 for any participation in conduct that may cause damage to submarine cables, as the maritime industry in Panama represents a significant proportion of the country's Gross Domestic Product (GDP) and has the largest ship registry in the world. ([11]) Beyond Panama, there are several flag States with large registries, such as Liberia, the Marshall Islands and the Bahamas, which are known to be more lenient in terms of the imposition of fines when compared to other countries. ([12])

([11]) Submarine Cable Regulations (2024), *Legal & Regulatory Matters Year in Review: Perspectives of Andrés Fígoli*.

([12]) *Ibid*.

2.1.3. Divergent approaches to the United Nations Convention on the Law of the Sea and their implications for infrastructure projects

The United Nations Convention on the Law of the Sea (UNCLOS), adopted in 1982, lays down a comprehensive regime of law and order in the world's oceans and seas, establishing rules that govern all uses of the oceans. As such, the Convention is rightly recognised as the constitution of the ocean. Its provisions reflect customary international law and are thus binding on all States, irrespective of whether they have acceded to the Convention or not. By establishing the legal order for seas and oceans, the Convention contributes to sustainable development as well as to the peace, security, cooperation and friendly relations among all nations.

It is also imperative that the sovereignty and sovereign rights of coastal States over their maritime zones, as established under UNCLOS, are respected and that all States act in good faith and with due regard for the rights, duties and freedoms of other States under the Convention. All members of the international community must abide by the fundamental principles and rules of the law of the sea and should refrain from any actions undermining regional stability and security.

Articles 87 and 112 of UNCLOS ([13]) stipulate that the laying and maintenance of submarine cables in the high seas is an inalienable right of all States. Furthermore, Article 79 establishes that States are also entitled to lay submarine cables on the continental shelf of another country (coastal State) and that this coastal State cannot impede it.

However, despite the fact that UNCLOS has been signed and ratified by 170 States as well as by the EU, thus constituting part of the EU acquis, a small number of States still remain non-parties to UNCLOS, some of which go even so far as to question the well-established fact that it reflects customary international law. States' violation of the international law, use or threat to use force against lawful maritime activities developed and supported in full respect of international law, including UNCLOS, have repercussions on the timely and effective development of undersea infrastructures of strategic importance for EU connectivity.

2.1.4. Issues pertaining to private law

The submarine cable industry relies primarily on installation and maintenance contracts to plan, deploy and maintain submarine cables. To address various issues that can occur during the planning, installation and maintenance of submarine cables, the industry has developed standard contract provisions governing the installation, transportation repair and other related services for submarine cables, which serve as best practice; these include:

- The International Federation of Consulting Engineers (FIDIC), which represents national associations of consulting engineers across the globe, has published such guidelines in its Yellow Book. ([14])

([13]) United Nations (1982), *United Nations Convention on the Law of the Sea*, Articles 87 and 112.

([14]) The Yellow Book (Conditions of Contract for Plant and Design-Build) is a suite of standard forms of contracts for use on international construction and engineering projects developed by FIDIC. The first edition of this book was published in 1999, with subsequent editions currently in force.

- The Norwegian Oil and Gas Association, a professional organisation and employer association for oil and supply companies, has also published its own local model, referred to as the Norwegian Subsea Contract NSC 05. ([15])

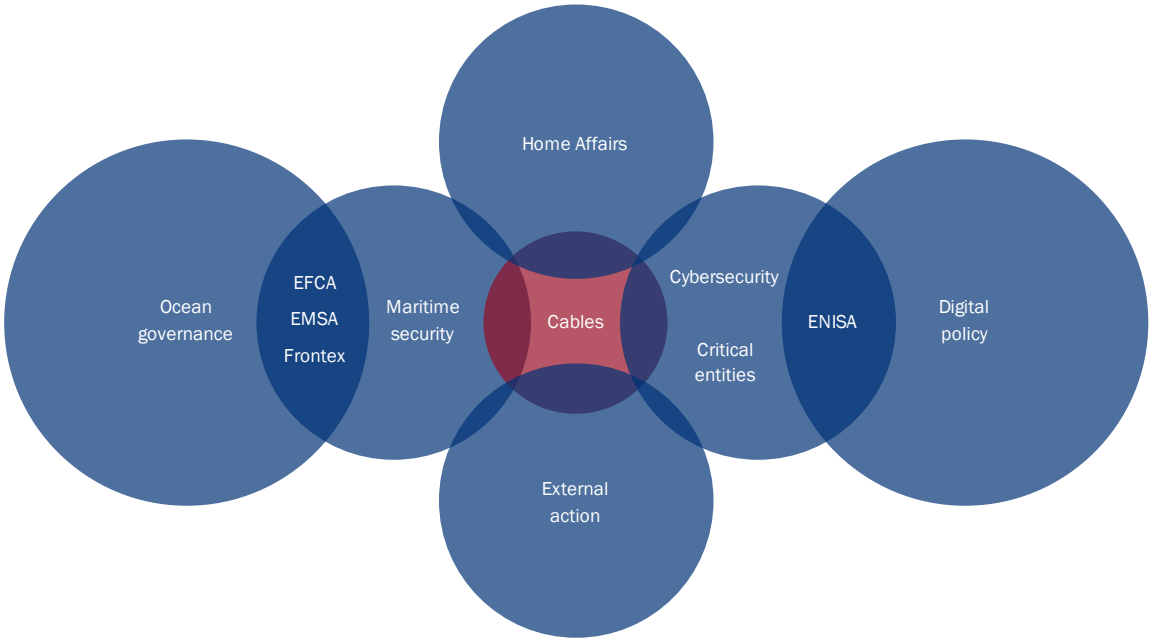
Although these contracts are non-binding and parties are not required to adhere to their standards, it is highly recommended that parties follow these guidelines to align with other industry participants. ([16])

2.2. EU

Submarine data cable infrastructure is addressed across several EU initiatives and policy processes, with differing degrees of emphasis and priority. At least five policy domains, driven by different EU bodies and agencies, are of relevance, as shown in Figure 2.2 below.

Issues related to cable security are most explicitly addressed within 1) maritime security and 2) cybersecurity policy. However, submarine cables also feature in 3) ocean governance and 4) digital policy. Moreover, they are a critical component in 5) external action, including development policy and security & defence policy.

Figure 2.2: Relevant EU policies and agencies for submarine data cables [Source: Analysys Mason, 2025]



EFCA = European Fisheries Control Agency

EMSA = European Maritime Safety Agency

Frontex = European Border and Coast Guard Agency

These are areas in which the protection and resilience of submarine data cable infrastructure is a concern, but not necessarily a priority. Moreover, each area is cross-cutting and presents its own complexities , involving diverse institutional dynamics. The role of several EU agencies is relevant in this domain, although none of them is explicitly tasked to address submarine data cable protection and resilience: these include the European Border and Coast Guard Agency (Frontex),

([15]) Offshore Norge (2005), *Norwegian Subsea Contract (NSC 05)*.

([16]) Daria Shvets (2020), *The International legal regime of submarine cables: a global public interest regime*, Phd Thesis.

the European Defence Agency (EDA), the European Environmental Agency (EEA), the European Fisheries Control Agency (EFCA), the European Maritime Safety Agency (EMSA) and the European Union Agency for Cybersecurity (ENISA).

2.2.1. Maritime security

Maritime security has been a key concern at EU level since the late 2000s. Initial attention was primarily on crime at sea, particularly piracy and human smuggling, as well as irregular migration. However, additional, diverse challenges were increasingly recognised. This led to a holistic approach to maritime security, as exemplified in the first edition of the European Union Maritime Security Strategy (EUMSS) and its action plan in 2014. In 2023, the EUMSS and its action plan were revised to ensure the EU has the tools to face new and evolving maritime security threats at its disposal, including growing strategic competition for power and resources in the sea basins around the EU and beyond, degradation of the marine environment, as well as attacks targeting critical maritime infrastructure.

The EUMSS and its action plan provide the framework for the EU to safeguard its interests at sea, protect its citizens and territory, and promote its values and economy. They reinforce the international rules-based order, ensuring compliance with international instruments, particularly UNCLOS.

The EUMSS also contains various actions designed to enhance the surveillance, protection and resilience of critical maritime infrastructure, including submarine data and electric cables. The Cable Action Plan notably refers to the Common Information Sharing Environment (CISE), which can play a crucial role in enhancing maritime domain awareness at EU level. CISE enhances the ability of Member States' relevant authorities and EU agencies (EMSA, EFCA and Frontex in particular) to exchange information relevant to the surveillance and protection of critical maritime infrastructure, securely and in real time. A provisional political agreement between the European Parliament and the Council to update the mandate of EMSA was reached in May 2025 to help bolster EMSA's role in cybersecurity, maritime security and other environmental issues. The EUMSS is being implemented on a voluntary basis by Member States, the EEAS and the European Commission ('the Commission'), with various EU agencies also involved. An implementation report will be presented by the High Representative of the Union for Foreign Affairs and Security Policy ('the High Representative') and the Commission in the fourth quarter of 2026.

EU agencies

EFCA, EMSA and Frontex are the three principal EU agencies involved in maritime security and, together, provide surveillance, information sharing and law-enforcement coordination functions, also known as coast guard functions. Their mandate and focus differ, as follows:

- **EFCA** oversees fisheries regulation and supports EU Member States in monitoring fishing activities, conducting inspections, ensuring compliance and facilitating information sharing. EFCA's mandate is relevant to the protection of submarine cable infrastructures because fishing vessels are a major cause of damage to submarine cables and, as such, is a key factor in the protection of submarine data cable infrastructure. ([17]) However, cable protection and surveillance are not explicitly included in current fisheries policies or compliance frameworks. That said, the issue has been raised at coast guard forums in which EFCA actively participates (discussed below).

([17]) European Parliament (2022), *Security threats to undersea communications cables and infrastructure*.

- **EMSA** assists EU Member States in matters of maritime safety. This includes support for ensuring compliance with international and European safety and security regulations appliable to ports and vessels. Among these are measures directly related to maritime security, such as the International Ship and Port Facility Security (ISPS) Code, which was adopted in response to international terrorism. EMSA's second core function involves the monitoring of maritime activity, primarily within European waters, while retaining global capabilities.

  EMSA develops a maritime situational picture for EU Member States and the other agencies. The picture is based on data from the Automated Identification System (AIS), which tracks the position and route of vessels, along with satellite imagery from the Copernicus system. EMSA fuses this location data and applies algorithms to detect suspicious and non-compliant behaviour, supporting maritime law-enforcement operations. The Commission has assigned the technical development and implementation of CISE for the maritime domain to EMSA, while it maintains the policy steering role. CISE became operational on 1 July 2024 ([18]) and serves as a decentralised platform for the exchange of maritime surveillance data. The substantial maritime surveillance capabilities developed by EMSA can be used to conduct surveillance of marine surface activities in strategic submarine cable locations. EMSA is fully aware that its tools could be employed to conduct maritime surveillance, but the agency does not currently have the mandate or staffing required to conduct such activities. ([17]) EMSA's mandate is currently under review by the Commission, led by the Directorate-General for Mobility and Transport (DG MOVE). A provisional agreement on EMSA's mandate was reached on 20 May 2025. ([19])

- **Frontex** focuses primarily on migration management, including countering irregular migration and cross-border crimes such as human trafficking and smuggling of human beings. Frontex is in charge of EUROSUR, an integrated framework that facilitates the exchange of information and operational cooperation within the European Border and Coast Guard, aimed at improving situational awareness and increase reaction capability for the purposes of border management. EUROSUR Fusion Services, such as aerial surveillance, constitute important sources of information of EUROSUR. EU Member States contribute to the system through a dedicated national coordination centre, with Frontex being responsible for fusing such data, including sources provided by EMSA. ([20]) Frontex also operates the Maritime Intelligence Community & Risk Analysis Network (MIC-RAN), which was set up in 2018 to facilitate the exchange of information, intelligence and crime statistics cross-border, and the dissemination of its risk-analysis products. MIC-RAN is designed to support "operational/strategic early warnings, risk alerts, risk profiles, overview reports, area/port analysis, and mapping of EU/regional maritime risks". ([21])

([18]) European Maritime Safety Agency (2024), *Common Information Sharing Environment (CISE) - Operational Phase.*

([19]) European Commission (2025), *The Commission welcomes provisional agreement on new European Maritime Safety Agency mandate.*

([20]) Ireland is not party to Frontex but is invited to participate by the Frontex Management Board in a non-voting capacity. As of May 2025, Ireland's annual request to participate in Frontex was approved. See Frontex (2025), *Management Board Decision 11/2025 on Ireland's request for the participation in Frontex activities in 2025 and its financial contribution for this participation*.

([21]) European Commission (2020), *Report on the implementation of the revised EU Maritime Security Strategy Action Plan*, SWD (2020) 252, p.27.

Since 2018, all three agencies have started to explore how they can better cooperate in the areas of information sharing and risk management. In particular, this has involved increasing awareness and harmonising the different types of data and methodologies employed by each agency, alongside the creation of a unified glossary of terms.

CISE provides a critical platform for enhancing intra-agency cooperation, particularly in the areas of information sharing, integration and dissemination of information from Member States. ([22])

Coast guard forums

Coast guard forums serve as another useful tool for enhancing maritime security, information sharing and coordination across EU entities and the Coast Guard authorities of Member States. The European Coast Guard Functions Forum (ECGFF) is the main platform within the EU in this regard, while other regional forums contribute to ensuring good coordination and sharing of promising practices between the EU's actors responsible for coast guard functions and the EU's maritime neighbours. These include the Mediterranean Coast-Guard Cooperation Forum, the Baltic Sea Region Border Control Cooperation, the North Atlantic Coast Guard Forum (NACGF) and the Arctic Coast Guard Forum (ACGF). Although these regional forums are not formally part of the EU institutional framework, they provide a valuable context to discuss relevant technical topics among practitioners in the field of coast guard functions, covering important security-related subjects, including cable security.

The ECGFF is a self-governing, non-binding, voluntary, independent and non-political forum that was created in 2009. It brings together the coast guard authorities from 25 EU Member States and Schengen-associated countries, as well as representatives of EU institutions and bodies with competencies related to EU coast guard functions to facilitate "co-ordination of work on specific aspects, such as maritime information sharing, cybersecurity, analysis of risks at sea and capacity building". ([23]) However, the ECGFF has not yet explicitly placed cable protection at the forefront of its agenda. As highlighted in the EUMSS implementation report, the Forum has significantly contributed to maritime cybersecurity through a series of workshops and dedicated working groups under the banner of the ECGFF, and involving ad-hoc governmental and private-sector stakeholders. ([24]) Given its ability to be a valuable place where practitioners can effectively address emerging issues and involve a broad range of relevant actors, the Forum could also serve as a valuable platform to discuss the subject of submarine cable resilience.

([22]) European Commission (2019), *Commission Staff Working Document. Review of the Common Information Sharing Environment (CISE) for the maritime domain: 2014 – 2019*, SWD (2019), 322.

([23]) European Commission (2025), *Coast guard cooperation*.

([24]) Because of the increasing cybersecurity challenges to both governmental and private-sector stakeholders in the maritime domain, cybersecurity requirements are widely integrated in new capability projects and regulations. Ensuring sufficient levels of cybersecurity is considered even more essential following the introduction to the maritime domain of emerging technologies such as autonomous vessels, blockchain, remotely piloted systems and the internet of things (IoT). Close coordination among key stakeholders at national level enables harmonisation of requirements and consistency in approaches (Italy, Lithuania, Portugal and Romania). The ECGFF working group on cyber-attack prevention has also been an important platform for cooperation between Member States seeking to develop common detection procedures and build a European network to fight cyber threats. Several countries (including Italy, Belgium, Croatia, Portugal, Finland and Spain) and EU agencies reported on their active participation in the workshops organised in 2019 under the Italian chairmanship73 of the ECGFF. These workshops sought to increase awareness, and exchange best practices and existing tools on risk management. See European Commission (2020), *Joint Staff Working Document. Report on the implementation of the revised EU Maritime Security Strategy Action Plan*, SWD (2020) 252.

Finally, the European Coast Guard Functions Training Network (the 'ECGF Training Network') is an association of education institutions providing education in the field of coast guard functions. The ECGF Training Network was established to develop joint curricula and foster a shared understanding of the essentials of coast guard operations, and also serves as a potential support mechanism not only for the work of the ECGFF, but also more broadly. To date, the ECGF Training Network has not developed course content addressing submarine cable dimensions, but could serve as a viable tool for enhancing awareness in this area.

2.2.2. Physical and cyber security of submarine cable infrastructures

Cybersecurity policy is the second main policy domain of relevance after maritime security. Over the past 10 years, cybersecurity has escalated to the top of the political agenda in the EU, and cybersecurity considerations have been embedded across multiple EU policy areas. Under Commission Presidency of Ursula von der Leyen, the preeminent position of cybersecurity has been confirmed. In her political guidelines for the 2019–2024 Commission mandate, the Commission President has underlined that "digitalisation and cyber are two sides of the same coin", which illustrates that cybersecurity is a top priority. ([25])

The first EU cybersecurity strategy was released in 2013, emphasising the importance of EU action "to counter cyber risks and threats having a cross-border dimension", by strengthening European cyber resilience. ([26]) The strategy came along with the first-ever proposal for EU cybersecurity legislation, namely the Network and Information Security Directive (the 'NIS Directive'), adopted in 2016, with a transposition deadline for Member States in 2018. ([27])

Subsequently, the EU's Cybersecurity Strategy for the Digital Decade was adopted in 2020, while the new NIS2 Directive ([28]) was officially approved in 2022. Among other aspects, the NIS2 Directive streamlines the regulatory framework by repealing provisions of the European Electronic Communications Code ([29]) (EECC) related to the security of networks and services, and to implementation and enforcement (Articles 40–41 of the EECC), the substance of which is covered by the NIS2 Directive. The deadline for Member States to transpose the NIS2 Directive passed in 2024.

Concurrently, policies related to the physical security of submarine cables have been elevated through strategic policy initiatives. The physical security of submarine cables refers to the protection of tangible infrastructure such as the cables themselves, landing stations and associated terrestrial components, from threats like sabotage, accidental damage and environmental hazards. The Critical Entities Resilience (CER) Directive is one such policy, mandating identified critical

([25]) European Commission (2019), *A Union that Strives for more. My agenda for Europe*, p.13.

([26]) European Commission (2016), *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013)*, p.5.

([27]) European Parliament and the Council of the European Union (2016), *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*.

([28]) European Parliament and the Council of the European Union (2022), *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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)*.

([29]) European Parliament and the Council of the European Union (2018), *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*.

entities to strengthen the resilience of their infrastructure. The Cable Action Plan complements the CER Directive, outlining a comprehensive approach through four key pillars.

These and other relevant policies are discussed further in the following subsections, which examine the main existing legislative and policy initiatives related to cybersecurity and resilience of critical infrastructure in the EU; these initiatives are presented in chronological order and include:

- the EU Cybersecurity Act ([30])
- the 'EU coordinated risk assessment of the cybersecurity of 5G networks' ([31]) report and the 5G Toolbox of risk-mitigating measures ([32])
- the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure ([33])
- the Network and Information Security Directive 2 (the 'NIS2 Directive') ([34])
- the CER Directive ([35])
- Recommendation (EU) 2024/779
- the Cyber Resilience Act ([36])
- the Cyber Solidarity Act ([37])
- the EU Action Plan on Cable Security ([38])
- ProtectEU – the European Internal Security Strategy. ([39])

It is important to highlight that the simultaneous adoption of the NIS2 and CER Directives, both of which entered into force in January 2023, marks a significant milestone, as both pieces of legislation establish a robust framework for protecting EU critical infrastructure from physical and cyber threats.

Each of these initiatives is discussed in turn below.

([30]) European Parliament and the Council of the European Union (2019), *REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*.

([31]) NIS Cooperation Group (2019), *EU coordinated risk assessment of the cybersecurity of 5G networks*.

([32]) NIS Cooperation Group (2020), *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*.

([33]) European Commission (2022), *Council Recommendation (2023/C 20/01) on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.*

([34]) European Commission (2022), *Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)*.

([35]) European Parliament and the Council of the European Union (2022), *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities*.

([36]) European Parliament and the Council of the European Union (2024), *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*.

([37]) European Parliament and the Council of the European Union (2025), *Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)*.

([38]) European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (2025), *Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security*.

([39]) European Commission (2025), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy*.

The EU Cybersecurity Act

In 2017, the EU adopted a set of policy proposals aimed at strengthening cybersecurity across Member States. It included a "Cybersecurity Act", revising the mandate of ENISA (notably to become a permanent mandate) and introducing a European system for cybersecurity certification to improve the security of networked devices and digital products and services. ([40]) The EU Cybersecurity Act was adopted in 2019. ([41]) Since then, ENISA gained a permanent status and has been involved in a broad range of cybersecurity initiatives across the EU, including policy development and implementation, certification and standardisation for Information and Communication Technology (ICT) products, services and processes, as well as capacity building and awareness raising. ENISA has been issuing annual reports on digital security incidents for the past 10 years. It also has also published many dedicated reports, including one that offered technical guidelines to assist national authorities in the supervision of submarine cables. ([42]) Additionally, ENISA has developed stress test guidelines, using submarine cables as an example case study to demonstrate how the guidelines can be applied in practice.

The EU Cybersecurity Act is expected to be revised soon, in an effort to strengthen the EU's resilience against rising cyber threats.

'EU coordinated risk assessment of the cybersecurity of 5G networks' and 'Cybersecurity of 5G networks EU Toolbox of risk mitigating measures'

In October 2019, the NIS Cooperation Group published a report on the EU co-ordinated risk assessment of the cybersecurity of 5G networks. ([43]) The report is based on the national risk assessments submitted by Member States to the Commission and, on this basis, identifies five risk scenarios related to insufficient security measures, the 5G supply chain, main threat actors, interdependencies between 5G networks and other critical systems, and end-user devices, including security requirements that are relevant to submarine cables.

The report serves as the foundation for the 'Cybersecurity of 5G networks EU Toolbox of risk mitigating measures', published by the NIS Cooperation Group in January 2020 ([44]) and endorsed by the Commission and the EU Member States. This toolbox provides strategic and technical measures to mitigate the identified risks, as well as supporting actions to reinforce their effectiveness. The strategic measures include enhancing regulatory powers to scrutinise network procurement and deployment, addressing non-technical vulnerabilities, and promoting a diverse 5G supply chain to avoid long-term dependency risks. The technical measures focus on strengthening the security of network equipment and processes which are applicable to submarine cables as part of the broader communications infrastructure. On 15 June 2023, the Commission adopted a 'Communication on the implementation of the 5G cybersecurity Toolbox (C(2023) 4049)', underlining strong concerns about the risks posed by certain suppliers and committing to implement the 5G toolbox to its own procurement of telecoms services, and when allocating EU funding.

([40]) European Commission (2018), *Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*, COM (2017), 477.

([41]) European Parliament (2019), *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*.

([42]) ENISA (2023), *Subsea cables - what is at stake?*

([43]) NIS Cooperation Group (2019), *EU coordinated risk assessment of the cybersecurity of 5G networks*.

([44]) NIS Cooperation Group (2020), *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*.

Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure

The Council of the European Union adopted the 'Council Recommendation on a Union-wide co-ordinated approach to strengthen the resilience of critical infrastructure' in December 2022. ([45]) The Recommendation is a non-binding act aimed at increasing coordination among Member States to identify and protect critical infrastructure across key sectors, including digital infrastructure and important cross-border critical infrastructure. It underscores the need for enhanced preparedness, a coordinated response and international cooperation to protect infrastructure that is vital to the EU's internal market and social stability, including submarine cables. It responds to growing concerns over external threats and hybrid campaigns that may affect critical European infrastructure, such as the Russia–Ukraine conflict.

The Recommendation identifies that several existing policies assign responsibility to Member States for securing critical infrastructure within their own jurisdictions, while noting the absence of policies that promote co-ordinated efforts across Member States. More specifically, the Recommendation encourages Member States to update risk assessments, conduct stress tests based on joint scenarios at the EU level, and leverage all tools available to strengthen the physical and cyber resilience of critical infrastructure. It explicitly acknowledges the strategic importance of submarine infrastructure, calling for increased attention to assets located outside national territories, such as submarine data cables. In terms of response, the Recommendation laid the groundwork for the Recommendation for a Critical Infrastructure Blueprint, adopted in 2024, which provides a roadmap for EU-level co-ordination during cross-border incidents. ([46]) This includes improving situational awareness, communication and operational readiness across sectors.

For submarine cables, the Recommendation reinforces the EU's commitment to proactive cross-border resilience planning. It complements other legal instruments like the NIS2 Directive and the CER Directive, creating a layered policy framework that addresses both the physical and cyber dimensions of submarine cable security.

The Network and Information Security Directive 2

In December 2022, the EU adopted the revised Directive on measures for a high common level of cybersecurity across the EU, known as the NIS2 Directive. ([47]) Among other provisions, the Directive sets out requirements regarding Member States' national cybersecurity strategies, including a requirement to adopt policies related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables. Moreover, national cybersecurity strategies have to include, *inter alia,* a mechanism to identify relevant assets and an assessment of risks in that Member State.

The NIS2 Directive, as part of the EU Security Union Strategy for the period 2020 to 2025, places strong emphasis on the protection and resilience of critical infrastructure, and outlines a framework that recognises the increasing interconnection between security challenges. ([48]) Besides mandating

([45]) European Commission (2022), *Council Recommendation (2023/C 20/01) on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.*

([46]) Council of the European Union (2024), *Council Recommendation on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance C/2024/4371*.

([47]) European Commission (2022), *Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)*.

([48]) European Commission (2020), *Communication from the Commission on the EU Security Union Strategy, 2020 to 2025*.

the adoption of national cybersecurity strategies, the NIS2 Directive requires Member States to designate or establish competent authorities, Computer Security Incident Response Teams (CSIRTs) and cyber crisis management authorities. It further sets requirements for essential and important entities in 18 critical sectors to report significant incidents and to adopt cybersecurity risk-management measures.

One of the critical sectors defined in the NIS2 Directive is the digital infrastructure sector, encompassing IXP providers, Domain Name System (DNS) service providers excluding operators of root name servers, Top-Level Domain (TLD) name registries, cloud computing service providers, data-centre service providers, Content Delivery Network (CDN) providers, trust service providers, providers of public electronic communications networks and providers of publicly available electronic communications services. Another critical sector is ICT service management (business-to-business), which encompasses managed service providers and managed security service providers. A third critical sector is digital providers, which encompasses providers of online marketplaces, providers of online search engines and providers of social networking services platforms.

The NIS2 Directive mandates that essential and important entities adopt cybersecurity risk-management measures such as risk analysis, information system security, incident handling and business continuity. As regards the aforementioned types of entities, with the exception of IXP providers, further details on the technical and methodological requirements of the risk-management measures are provided in a Commission Implementing Regulation, ([49]) which, among other elements, addresses environmental and physical security, including the monitoring of environmental parameters, where appropriate. Management bodies of essential and important entities have to approve those entities' cybersecurity risk-management measures and oversee their implementation, which means that the entities not only need to secure their networks, but also embed cybersecurity into their organisational culture.

The NIS2 Directive also facilitates cross-border cooperation to facilitate coordinated responses to large-scale cyber incidents. Furthermore, it provides a legal basis for the NIS Cooperation Group to conduct Union-level coordinated security risk assessments of critical supply chains. By setting out measures for a high common level of cybersecurity across the EU, the NIS2 Directive enhances the EU's ability to safeguard its digital backbone.

The Critical Entities Resilience Directive

Alongside the NIS2 Directive, the EU co-legislators adopted the Critical Entities Resilience Directive (the 'CER Directive'), which lays down obligations on EU Member States to take specific measures to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market. ([50]) The CER Directive covers 11 sectors including energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space, as well as production, processing and distribution of food. The CER Directive states that

([49]) European Commission (2024), *Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers*.

([50]) European Commission (2022), *Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC*.

critical entities must have a comprehensive understanding of the relevant risks to which they are exposed and are obliged to assess those risks. To that end, critical entities, once identified as such, must carry out risk assessments in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment'), repeating risk assessments whenever necessary subsequently, and at least every 4 years.

The entities identified as critical under the CER Directive are automatically considered essential under the NIS2 Directive. ([51]) This ensures that the entities are required to meet both the physical resilience obligations under the CER Directive and cybersecurity obligations under the NIS2 Directive. Furthermore, the CER Directive includes provisions to avoid duplication of obligations for critical entities in the digital infrastructure sector. For example, Article 11 and Chapters III, IV and VI of the CER Directive do not apply to digital infrastructure entities to reduce the administrative burden. ([52]) More specifically:

- Article 11 requires Member States to consult and coordinate on ensuring the physical security of critical entities where the critical infrastructure or part of the corporate structures is connected between two or more Member States, or a critical entity identified in one Member State provides essential services to or in another Member State.

- Chapter III requires Member States to ensure critical entities conduct risk assessments within the required timeline as per Article 6 (3) of the CER Directive (i.e., within 9 months of receiving the notification from the Member State and every 4 years). In addition, critical entities are required to implement mitigation measures to reduce the impact of the identified risks and notify the competent authority of any incidents that have had a significant impact on the provision of essential services.

- Chapter IV sets out the parameters for which an entity is identified as a critical entity of significance. Entities must already be identified as critical entities following Article 6(1) of the Directive, must provide similar essential services in six or more Member States and must be notified through the Member State's competent authority. Member States are required to create an advisory mission to assess the mitigation measures in place, as per Chapter III.

- Chapter VI outlines the powers provided to competent authorities in ensuring that critical entities follow the requirements of the CER Directive and the means to require the entities to carry out these measures. Competent authorities may conduct inspections, issue binding instructions and, in the case of non-compliance, impose penalties, among other measures.

Recommendation (EU) 2024/779

In February 2024, the Commission published 'Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures'. ([53]) The Recommendation establishes a policy coordination framework which outlines a set of actions at national and EU level aimed at improving the security and resilience of submarine cable infrastructures through better co-ordination across the EU, both in terms of governance and funding. This Recommendation is also a response to the 'Council Recommendation of 8 December 2022 on a Union-wide co-ordinated approach to

([51]) European Commission (2022), *Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)*, Article 3(1)(f).

([52]) Commission for Communications Regulation in Ireland, *CER Directive*.

([53]) European Commission (2024), *Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures*.

strengthen the resilience of critical infrastructure (2023/C 20/01)', ([54]) which invited the Commission to carry out studies concerning the resilience of submarine cables, and called for more frequent risk assessments and stress tests on the cybersecurity and physical security of submarine cable systems.

In the same month, the NIS Cooperation Group also published a 'Report on the cybersecurity and resiliency of the EU communications infrastructures and networks', ([55]) as a follow-up to a meeting in Nevers (France) in March 2022. During that meeting, the EU ministers in charge of telecoms had unanimously adopted the Nevers Call to reinforce the EU's cybersecurity capabilities (hereafter referred to as the 'Nevers Call') and identified telecoms networks as "prime target[s]" for cyber-attacks. ([56])

The follow-up report to the Nevers Call identifies a number of threats for communications networks, as well as their vulnerabilities. It also presents a series of risk scenarios of strategic importance for the EU, and provides strategic and technical recommendations to mitigate these risks, which are, to a large extent, applicable to the present report.

The protection of submarine cables is dependent on the regulatory regime in each Member State. With the transposition of the European Electronic Communications Code (EECC) by each Member State into national law, ([57]) telecoms providers are obliged to report incidents that have a significant impact on the operation of networks or services to their competent national authorities. This may involve reporting incidents affecting submarine data cables; however, the implementation of the regulation, the ownership and operating structures of the submarine data cable infrastructure, its cross-border coordination and the partially non-national location of such infrastructure make the current submarine data cable incident-reporting process ambiguous. The incident-reporting and cybersecurity risk-management provisions from the EECC were incorporated into the more recent, comprehensive NIS2 Directive and, therefore, the corresponding EECC Articles 40–41 were repealed (see above).

The Cyber Resilience Act

The Cyber Resilience Act (CRA) entered into force in December 2024. ([58]) It mandates that manufacturers of products with digital elements (software and hardware) intended for the EU market adhere to security-by-default and security-by-design principles, which must be maintained throughout the lifecycle of the products. The Act covers a wide range of products, including those used in submarine cable infrastructures such as routers and switches.

([54]) European Commission (2022), *Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.*

([55]) European Commission (2024), *Report on the cybersecurity and resiliency of the EU communications infrastructures and networks*.

([56]) European Commission (2024), *Report on the cybersecurity and resiliency of the EU communications infrastructures and networks*.

([57]) European Commission (2018), *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*.

([58]) European Parliament and the Council of the European Union (2024), *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*.

By improving the cybersecurity of products placed in the internal market, the CRA contributes to increasing transparency and enhancing security at every stage of the supply chain for critical infrastructure, as covered by the NIS2 Directive. The main obligations introduced by the Act will apply from 11 December 2027.

The EU Cyber Solidarity Act

The EU Cyber Solidarity Act entered into force in February 2025. ([59]) It aims to strengthen detection, preparation and response capacities in the EU against significant and large-scale cybersecurity threats and attacks. The Act proposes the creation of a network of interconnected Security Operation Centres (SOCs) across the EU, facilitating better monitoring and response to threats, including those affecting submarine cables.

These frameworks and measures collectively contribute to the security and resilience of submarine cables, ensuring they are protected against both physical and cyber threats.

The EU Action Plan on Cable Security

In February 2025, the Commission and the High Representative issued the 'EU Action Plan on Cable Security' (the 'Cable Action Plan') ([60]) to enhance the security of submarine cable infrastructures. The Cable Action Plan sets out four priorities to secure critical infrastructure for both communication and energy submarine cables, focusing on prevention, detection, response and repair, as well as deterrence.

The first objective of the Cable Action Plan **is to prevent** any disruptive incidents and increase the resilience of submarine cable infrastructures against potential threats and vulnerabilities. The Plan outlines a number of preventive actions, which are expected to be implemented by the fourth quarter of 2025; these include:

- mapping of existing and planned submarine cable infrastructures
- coordinating risk assessments (risks, vulnerabilities and dependencies) on submarine cables, taking into account spare part security of supply, and stress testing methodology
- creating a Cable Security Toolbox of mitigating measures
- developing a priority list of Cable Projects of European Interest (CPEIs).

The present report addresses these four actions. To facilitate increased prevention of disruptive incidents, the Commission will propose a Delegated Act to amend Annex V of the Connecting Europe Facility (CEF) regulation to prioritise CPEIs as CEF Projects of Common Interest, which will be the first step towards creating an EU Investment Framework for submarine cable projects.

As a second objective, the Cable Action Plan urges the EU to increase its **detection** capacity to identify and anticipate threats as early as possible. Currently, the EU cannot effectively monitor the threats that affect submarine cable infrastructures. In addition, although there are a number of maritime surveillance and situational awareness systems already in place, such as EMSA's Integrated Maritime Services system, there is a lack of integration of these systems at the EU level. As such, the Cable Action Plan outlines the following key actions on detection:

- supporting the development of a voluntary integrated surveillance mechanism for submarine cables per sea basin

([59]) European Commission (2025), *The EU Cyber Solidarity Act.*

([60]) European Commission (2025), *Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security*.

- working towards the rapid establishment of a dedicated regional hub in the Baltic Sea region as a test bed
- exploring the concept of a network of submarine sensors to be deployed to secure submarine cables
- launching a dedicated surveillance drones programme (air, surface and underwater)
- preparing a report to promote the use of new technological solutions for detection of cable incidents
- supporting the development of public–private partnerships with cable operators for voluntary reporting of cable incidents.

Furthermore, the Cable Action Plan considers that the use of Science Monitoring and Reliable Telecommunications (SMART) cables with integrated sensor and monitoring systems is crucial for detecting threats to submarine cables. It recognises the promotion of sensor and monitoring technologies in CEF regulation to promote the identification of threats to submarine cable infrastructure. The Cable Action Plan has called for the "design of an industrial roadmap for the deployment of surveillance and protection technologies for submarine cable infrastructures" by establishing an industry forum with relevant stakeholders. ([61])

In the event of an incident affecting a submarine cable, the third objective of the Cable Action Plan is to **respond** as quickly as possible to **repair** the damaged submarine cable in a coordinated way, in solidarity with the Member States that are most affected by the disruption. The recent incidents in the Baltic Sea have highlighted the need for increased coordination and synergy between different crisis management frameworks, and for effective use of the existing incident-reporting mechanisms set out in the CER and NIS2 Directives. As such, the Cable Action Plan establishes the following key actions on response and recovery:

- enhance the effectiveness of the EU's response to crisis by increasing synergies with existing frameworks
- pool a budget from EU funding programmes, including the possibility for voluntary transfers by Member States from cohesion funds into the CEF, to finance an increase in the capacities of EU cable vessels, as well as modular repair equipment
- propose to build an EU cable multipurpose Vessels Reserve in the medium term, depending on the needs; this could be complemented by regional framework agreements to secure the availability of appropriate vessels with crews
- design a joint approach to ensuring the security of supply of cable spare parts through, for example, targeted stockpiles.

The fourth and final priority established in the Cable Action Plan is **deterrence**, to reduce the likelihood of further incidents, by holding malicious actors accountable for their actions and raising the costs for such actors. As such, the Commission, in cooperation with Member States, will:

- deploy a proactive cable diplomacy to reach out to strategic partners, including in multilateral fora, with a view to cooperate on issues related to cable security
- enhance the capacities of the EU to react to and limit the impact of threats and threat actors in line with international law
- enhance the capacity to hold malicious actors accountable, by making best use of the existing sanction regimes
- step-up the strategic communication approach on cable security to combat the hybrid campaign abusing plausible deniability

([61]) European Commission (2025), *EU Action Plan on Cable Security*, Section 2.2.3.

- launch a reflection to make full use of the International Law of the Sea framework to enhance the security of submarine cables
- reinforce dialogue and co-operation with NATO on cable security.

ProtectEU

In April 2025, the Commission presented ProtectEU – the European Internal Security Strategy, which aims to increase the capabilities of EU Member States to protect societies and democracies from online and offline threats from terrorists, criminals and hostile foreign actors. ([62]) ProtectEU emphasises the growing threat landscape where threats such as cyber intrusions, sabotage and disinformation target critical infrastructure assets. It notably calls for enhancing resilience against hybrid threats and other hostile acts, underlining that the timely transposition and correct implementation by all Member States of the CER and NIS2 Directives is crucial. Following successful stress tests in the energy sector in 2023, the Commission will promote voluntary stress tests in other key sectors for internal security. Submarine cables, which underpin Europe's digital connectivity and economic stability, are explicitly recognised as vulnerable to such threats. As outlined in the Cable Action Plan, the Commission recalls the need for enhanced situational awareness and integrated surveillance mechanisms, as well as multi-stakeholder cooperation involving law enforcement, cybersecurity agencies, private operators and international partners such as NATO. ([63])

Furthermore, ProtectEU advocates for the integration and mainstreaming of security considerations across all EU legislation, policies and programmes, including EU external action.

2.2.3. The broader policy context

Maritime security and cybersecurity are the primary policy areas in which the resilience of submarine data cables plays a critical role. However, a broader policy context provides valuable insights into potential opportunities to enhance the security of submarine cable infrastructures at the EU level, as well as associated challenges.

Ocean governance and maritime policy

Submarine cables are an issue within the EU's broader ocean governance and maritime policy, since they are physically located on the seabed. The EU's Integrated Maritime Policy of 2007, ([64]) supported by the Commission's 2012 Blue Growth strategy, ([65]) emphasises the importance of marine spatial planning and marine surveillance with a global outlook. Additionally, the Commission's joint communication of 10 November 2016 on international ocean governance ([66]) identifies different maritime crimes as a major challenge and lays down the global maritime

([62]) European Commission (2025), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy*.

([63]) European Commission (2025), *Joint communication to the European Parliament and the Council on the EU Action Plan on Cable Security, 2025/9*.

([64]) European Parliament (2025), *Integrated maritime policy of the European Union*.

([65]) European Commission (2012), *Blue Growth opportunities for marine and maritime sustainable growth*.

([66]) European Commission (2016), *International ocean governance: an agenda for the future of our oceans*.

ambitions of the EU. It also stresses the need for integrating different policies and engaging in international cooperation and capacity building.

None of these policies explicitly mentions cables. However, they provide an important framework for the EU's maritime agencies and devise ocean governance tools that are prospectively useful for the protection of submarine cables, notably through facilitating maritime surveillance and promoting marine spatial planning.

One of the primary goals of ocean governance policies is to expand marine protected areas. Marine activities are very restricted in marine protected areas, which diminishes the risk of incidents to submarine cables. Since cable installations have a very limited environmental impact once installed, there is a strong synergy between the objectives of marine protection and data cable resilience. Indeed, analysts have highlighted that **cable corridors within marine protected areas are a potential solution to enhance cable resilience**. ([67]) Hence, there are potential synergies between marine protection and cable resilience, and the European Environmental Agency could have a prospective role in this regard. It should be noted, however, that while the rationale behind using cable corridors as a potential solution can be beneficial to prevent unintended damage, it could be detrimental to the resilience of submarine cables, as all cables are effectively concentrated in a single narrow corridor and, consequently, are easier to target collectively.

Digital policy and infrastructure

As digital development progresses, technologies from foreign companies and States are becoming increasingly integrated into both the everyday life of European citizens and the daily operations of European critical infrastructure. In response, the EU has come to view external influence and dependencies as a potential security threat, and is seeking to reclaim control over critical technologies and infrastructure. This has led to calls for achieving European digital sovereignty based on retaining and retaking control of data, technologies and infrastructure.

To this end, the Commission has adopted a range of digital policy initiatives, including strategies on Artificial Intelligence (AI), data, the digital future, the European industry and the European Data Gateway Platforms Strategy. ([68])

Response to hybrid threats

The 2016 'Joint Framework on countering hybrid threats' provides another important instrument for building cable resilience. ([69]) It established the EU Hybrid Fusion Cell as part of the EU Intelligence and Situation Centre (EU-INTCEN), which provides an important analytical capability for developing scenarios and enhancing information exchange on hybrid threats. The work has included maritime and transport security issues. It serves as an important instrument for collaboration between the EU and NATO, in particular to facilitate joint planning and exercises.

([67]) Carter, L. et al. (2009), *Submarine Cables and the Oceans: Connecting the World*, UNEP-WCMC Biodiversity Series, No. 31.

([68]) Bueger,C., Liebetrau, T. and Franken, J. for the European Parliament (2022), *Security threats to undersea communications cables and infrastructure – consequences for the EU*.

([69]) European Commission (2016), *Joint Communication to the European Parliament and the Council on a Joint Framework on countering hybrid threats a European Union response*.

The European Centre of Excellence for Countering Hybrid Threats, based in Helsinki, serves as an additional instrument in this collaboration. The Centre regularly provides analysis and guidance documents, and acts as a platform for discussing challenges. ([70]) In 2018, it hosted an event about maritime security, established a maritime network to improve maritime resilience and develop a shared understanding of vulnerabilities across three strands (ports, shipping and underwater cables). ([71])In its working paper series, cable failure is identified as one of several hybrid threat scenarios in the maritime domain. ([72])

The future of European competitiveness

The 2025 Competitiveness Compass for the EU sets out a roadmap for restoring Europe's dynamism and boosting economic growth. ([73]) It builds on Mario Draghi's independent report on 'The future of European competitiveness', published in September 2024, which highlights three key areas for action to help ignite sustainable growth across Europe: ([74])

- First, the EU needs to close the innovation gap with the US and China, as research and development (R&D) and innovation are the main drivers of growth in developed economies. The EU spends significantly less in R&D than the US, and R&D investments have primarily focused on the automotive and pharmaceutical industries. For the US, however, the main focus has been on the technology industry, which has led to the emergence of hyperscalers. Part of the problem is converting the innovation into a commercial product and, as such, many researchers are driven to relocate to the US for better funding and commercialisation opportunities. The report argues that, while it is too late to emulate hyperscalers in Europe, there is a need to unlock the innovation potential and lead investment in new technologies, as well as give Europeans the skills they need to commercialise these technologies.
- Secondly, there is a need to focus on decarbonisation and competitiveness. The net-zero targets set by the Commission have helped to drive decarbonisation, however, energy prices in the EU are still higher than in the US. A contributing factor is the lack of natural resources in the EU, and even with increased access to green energy, households still have not fully accessed the benefits of low-cost green power. The EU is a leader in clean energy, and one fifth of sustainable technologies worldwide are developed in the EU. However, the EU is not taking advantage of this opportunity. China is becoming highly competitive in clean technology and electric vehicles, while the EU is highly dependent on China as a cheaper and more efficient route to its decarbonisation targets. Decarbonisation can therefore become a source of growth for Europe with a joint plan spanning industries.
- Finally, the EU needs to increase its security while reducing dependencies on other nations. Europe is vulnerable to geopolitical risks due to its reliance on non-EU suppliers – such as

([70]) You can subscribe to the *Hybrid CoE newsletter* here.

([71]) Hybrid CoE (2018), *Network on Maritime vulnerabilities and resilience launched*.

([72]) Lohela, T. and Schatz, V. (2019), *Hybrid Coe Working Paper 5: Handbook On Maritime Hybrid Threats — 10 Scenarios and Legal Scans*.

([73]) European Commission (2025), *Communication from the Commission to the European parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions A Competitiveness Compass for the EU*.

([74]) European Commission (2024), *The Draghi report: A competitiveness strategy for Europe (Part A).*

China – for raw materials, particularly those used in the clean energy industry and for digital technology. In the case of submarine cables, certain components are not manufactured by any single European supplier, as outlined in Section 3.2.2. Draghi particularly references the need for a 'statecraft', including establishing co-ordinated preferential trade agreements with resource-rich countries, building up stockpiles in selected critical areas and securing the supply chain of key technologies, all of which are relevant recommendations to increase the security of submarine cables in Europe.

Strengthening Europe's preparedness and readiness

There are several ways in which the EU can enhance the security and resilience of its critical infrastructure. In March 2025, the EU put forward a European Preparedness Union Strategy, ([75]) which builds on the analysis and recommendations by Sauli Niinistö, in his capacity as special adviser to the President of the Commission, in a report published in October 2024. ([76]) As regards submarine cable security and resilience, Niinistö's points were addressed through the already mentioned Cable Action Plan. According to Niinistö, there are a number of ways to address key areas of vulnerability and dependency on third parties:

- Firstly, there is a call to assess and improve the resilience of international interconnections, including submarine cables, and to clarify the responsibilities of national authorities in protecting critical infrastructure. This will help to ensure robust and reliable connectivity even in the face of disruptions.
- Additionally, there is a need for greater transparency in the supply chain, particularly regarding suppliers and managed service providers. By mapping out these dependencies, authorities can better identify and mitigate potential risks.
- The recommendations also highlight the importance of fostering operational collaboration through regular cyber exercises and improving situational awareness and information sharing among operators. This collaborative approach will enhance the sector's ability to respond to and recover from cyber threats.
- Furthermore, the recommendations emphasise the need to extend physical stress testing to include digital infrastructure, ensuring that critical assets are prepared for both cyber and physical threats.

The technical recommendations focus on enhancing the cybersecurity measures and operational resilience of Europe's communications infrastructure:

- The recommendations call for the development of comprehensive technical guidelines to protect and enhance the resilience of submarine cables against both physical and cyber threats. This involves securing cable landing points, monitoring for potential sabotage and ensuring rapid repair mechanisms are in place.
- Exchanging good practices among stakeholders is also crucial. This includes sharing effective measures for protecting submarine cables, ensuring redundancy and implementing robust monitoring systems.

([75]) European Commission (2025), *Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy*.

([76]) Niinistö, S. (2024), *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*.

- Enhancing physical security also remains a priority, alongside ensuring the availability of repair vessels capable of addressing damage quickly.
- Improving situational awareness is essential. Operators and national authorities should implement real-time monitoring systems to detect and respond to threats promptly.
- Collaboration with international partners is also vital given that submarine cables often span international waters. This includes coordinating security measures, sharing threat intelligence and establishing clear protocols for responding to incidents affecting multiple countries.
- Finally, regular stress tests should be conducted to assess the resilience of submarine cables against various threat scenarios. These tests will help to identify vulnerabilities and ensure that appropriate mitigation measures are in place.

Economic security policy

The European Economic Security Strategy, introduced in June 2023, is a comprehensive framework designed to enhance Europe's economic security. ([77]) The aim of the strategy is to reduce risks arising from geopolitical tensions and shifts in technology that negatively affect the European economy.

A focus of the strategy is the proposal for the Commission and Member States to conduct risk assessments for the identification of common risks. The risk assessments cover similar issues outlined in the CER and NIS2 Directives, which include risks to the resilience of supply chains, risks to the physical and cybersecurity of critical infrastructure, technology security and technology leakage risks, and the risks of weaponizing economic dependencies. In addition, the strategy proposes three main pillars, namely promoting European competitiveness, protecting against commonly identified economic security risks, and creating partnerships with countries facing similar economic issues. ([78])

The strategy was updated in January 2024 to include five new initiatives, namely improving the screening of foreign investment into the EU, increasing the coordination of export controls, identifying potential risks from outbound investments in specific technologies, supporting research and development of dual-use technologies, and enhancing research security at national and sector level. ([79])

Although the strategy does not directly regulate submarine cables, it does influence the broader policy ecosystem surrounding them. With the NIS2 and CER Directives covering the physical and cybersecurity aspects, the strategy brings in the economic security of critical infrastructure such as submarine cables which is essential for digital connectivity, and upholds the economic flow of goods, services and finances. The aim of reducing reliance on non-EU suppliers follows other similar sentiments highlighted in the Nevers Report, among others. Finally, the goal of promoting technological sovereignty indirectly supports European vendors, while protecting these vendors from foreign investments that may pose a risk to their security or autonomy.

([77]) European Commission (2023), *Joint communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy"*.

([78]) European Commission (2023), *An EU approach to enhance economic security*.

([79]) European Commission (2024), *Commission proposes new initiatives to strengthen economic security*.

2.2.4. External action

External action is essential to strengthening the resilience of submarine cable infrastructures, given the transnational structure of the network, with a focus on nodal points and the countries to which the EU is connected, as well as the potential impact of cable failure on peace and security in the Global South. ([80])The recently published ProtectEU Internal Security Strategy makes the link with external threats, highlighting that internal security is increasingly influenced by external actions and the need to protect strategic infrastructure such as submarine cables against hybrid threats.

Neither the European Consensus on Development, adopted in 2017, ([81]) nor the EU's Global Strategy for Foreign and Security Policy ([82]), adopted in 2016, directly refers to submarine data cables, albeit underscoring the importance of critical infrastructure and maritime security. The EU Security Union Strategy, launched in 2020, ([83]) and the Strategic Compass, approved in 2022, ([84]) strongly emphasise digital infrastructure protection, both in physical and cyber terms. The 2023 EU Maritime Security Strategy also includes the protection of critical maritime infrastructure. These policy documents do not include a detailed action on submarine data cables, however, they indicate awareness of the issue. Furthermore, the EU's Global Gateway Communication, issued in 2021, ([85]) and the International Digital Strategy for the EU, adopted in 2025, ([86]) both recognise submarine cable infrastructures as a strategic priority. The following subsection offers a detailed review of strategies and activities that provide opportunities to embed cable resilience into external action.

International partnerships

In its introduction to international development partnerships under the resilience, peace and security theme, the EU hints at the topic when it stresses the objective to "mitigate global and emerging threats, such as terrorism and violent extremism, transnational organised crime (including environmental crime, illicit trafficking and cybercrime), protection and resilience of critical infrastructure (including public, maritime, air and cyberspaces) – as multipliers of global security challenges". ([87])

([80]) Global South refers to developing economies and generally includes Africa, Latin America and the Caribbean, most of Asia (excluding Israel, Japan and South Korea), and Oceania (excluding Australia and New Zealand).

([81]) European Commission (2017), *THE NEW EUROPEAN CONSENSUS ON DEVELOPMENT 'OUR WORLD, OUR DIGNITY, OUR FUTURE'. JOINT STATEMENT BY THE COUNCIL AND THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES MEETING WITHIN THE COUNCIL, THE EUROPEAN PARLIAMENT AND THE EUROPEAN COMMISSION*.

([82]) European Commission (2016), *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign And Security Policy*.

([83]) European Commission (2020), *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions On The Eu Security Union Strategy*.

([84]) European Union External Action (2020), *A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security*.

([85]) European Commission (2021), *The Global Gateway*.

([86]) European Commission (2025), *An International Digital Strategy for the European Union*.

([87]) European Commission (2025), *Peace and security*.

Under the theme of digital partnerships, ([88]) the Commission, in particular, works with the African continent to enhance digital infrastructure, which includes the development of cable networks (for example, under the AfricaConnect project). ([89]) Many countries in North Africa are nodal States for European cable connection.

As part of this, the EU has introduced a strategy to leverage AI and digital technologies to boost its competitiveness and security on a global scale. The International Digital Strategy for the European Union (JOIN(2025) 140 final) ([90]) highlights the need for the EU to work with international partners and allies to support mutual digital transitions, including shaping global digital governance to align with the EU's interests and values. The EU has already developed strong partnerships with a number of partners beyond the UK and outside of NATO. These include the Trade and Technology Councils with the US and India, digital partnerships with Japan, South Korea, Singapore and Canada, and Digital Dialogues with Brazil, Mexico, Argentina, Australia and the Western Balkans. ([91]) In addition, the EU maintains cyber dialogues with a number of countries including Ukraine, and comprehensive and strategic partnerships with countries such as Tunisa, Egypt and Jordan.

Furthermore, the EU continues to develop new free trade agreements and digital trade agreements to set digital trade rules for secure digital environments. As an example, on 3 September 2025, the Commission put forward the EU-Mercosur Partnership Agreement (EMPA) and the EU-Mexico Modernised Global Agreement (MGA) for signature and adoption, and both partnerships are expected to generate billions in trade opportunities. ([92]) Submarine cables are fundamental to building secure and resilient digital networks and infrastructures, which can be achieved through the aforementioned partnerships.

Foreign policy instruments

Under the Instrument contributing to Stability and Peace (IcSP) and through the Neighbourhood, Development and International Cooperation Instrument (NDICI), the EU runs important global capacity-building programmes in maritime security and ocean governance. There are also discussions within the UN Office on Drugs and Crime's (UNODC) Global Maritime Crime Programme that have addressed the cable resilience of small States in the Western Indian Ocean region. ([93])

([88]) European Commission (2025), *Digital partnerships*.

([89]) European Commission (2019), *AfricaConnect*.

([90]) European Commission (2025), Joint Communication to the European Parliament and the Council. An International Digital Strategy for the European Union.

([91]) European Commission (2025), Joint Communication to the European Parliament and the Council. An International Digital Strategy for the European Union.

([92]) European Commission (2025), *Commission proposes Mercosur and Mexico agreements for adoption*.

([93]) United Nations Office on Drugs and Crime (2019), *Key actions to protect submarine cables from criminal activity identified at UNODC global expert meeting*.

EU diplomacy

Diplomacy is crucial in managing relations with the two nodal States (Egypt and Morocco) and with the vast range of connected States in the North Atlantic (US, Canada and Norway), South Atlantic (Brazil and West Africa), the Mediterranean region (for example, Tunisia and Israel) and the Indo–Pacific region.

The European External Action Service started its cable diplomacy, reaching out to partners and like-minded countries. These partners are equally concerned about the security and resilience of critical maritime infrastructures, as incidents affecting submarine cables have taken place in other regions, such as West Africa, the Red Sea and the South China Sea, underlining the collective dependence on these infrastructures. Concretely, cable security was introduced as an item in the EU's existing foreign and security policy partnership formats, such as security and defence dialogues, as well as consultations and cooperation mechanisms, including in multilateral formats, for instance, with partners in the Association of Southeast Asian Nations (ASEAN) and the Indo-Pacific region (for example, under the 'Enhancing security cooperation in and with Asia' (ESIWA) project). The EU, for instance, supported the 5th ASEAN Regional Forum (ARF) Workshop on Implementing UNCLOS and other International Instruments to Address Emerging Maritime Issues, held in Hanoi in November 2023.

Moreover, regional strategies emphasise connectivity and infrastructures as key dimensions. It is worth noting that the EU joined the Memorandum of Understanding (MoU) on the protection of critical undersea infrastructure in the Baltic Sea at the ministerial meeting of the Council of the Baltic Sea States on 15–16 May 2025 in Estonia. This MoU sets out a framework for closer cooperation and support to the ten interested countries (eight EU Member States as well as Norway and Iceland). One of the actions under this framework will be the establishment of a network of designated points of contact.

As another example, 'The EU strategy for cooperation in the Indo-Pacific' ([94]) emphasises the importance of infrastructure, connectivity and digital partnerships, but does not assign an immediate action to submarine cables. Cable security is further referred to in the 'Joint Communication on a stronger EU engagement for a peaceful, sustainable and prosperous Arctic', issued in October 2021, ([95]) and the 'Joint Communication to the European Parliament and the Council – The European Union's strategic approach to the Black Sea region', published in May 2025. ([96])

A further important development is the potential contribution of the three ongoing EU CSDP naval operations (IRINI, ASPIDES and ATALANTA) to gather information on the protection of critical maritime infrastructure and the shadow fleet.

[94] European Commission (2021), *Joint Communication To The European Parliament And The Council. The Eu Strategy For Cooperation In The Indo-Pacific*.

[95] Available here.

[96] Available here.

Military coordination, the European Defence Agency and the Permanent Structured Cooperation

In the area of military and defence coordination, submarine data cables have been a recurring point of consideration in the EU Military Committee's discussions on maritime security. For instance, under the 2021 Portuguese presidency of the Council of the EU, maritime security events addressed the topic of submarine data cables. ([97]) Furthermore, the Ministerial Declaration on Data Gateways of March 2021 called for supporting actions to improve "the security, stability and resilience of the open internet on which our economy and society depends". ([98])The Strategic Compass, a major initiative in EU defence planning, also incorporates a significant maritime component, focusing on the resilience of critical maritime infrastructure. ([99]) However, submarine cables are not explicitly referenced in the final version of the Strategic Compass (although they are mentioned in the previously cited Global Gateway Communication).

In line with the objectives offset out in the EU Maritime Security Strategy, adopted in 2023, live Maritime Security Exercises (MARSEC) in 2024 (in Spain) and 2025 (in Italy) addressed the protection of critical maritime infrastructure, with the participation of a number of EU Member States, EU agencies (Frontex, EFCA and EMSA) and, in 2025, NATO observers.

Within the framework of the European Defence Agency (EDA), the Maritime Surveillance (MARSUR) project, launched in 2006, has contributed to developing a recognised maritime picture for European navies and facilitates military information exchange through the MARSUR Exchange System. ([100]) The system is intended to provide a military layer to CISE and could play an instrumental role, especially in relation to the surveillance of cables and suspicious activity on the high seas. Other relevant EDA projects include the European Unmanned Maritime Systems for Mine-Counter Measures and other naval applications, the Unmanned Maritime Systems (UMS) and the Maritime Mine CounternMeasures (MMCM) programme. Furthermore, CapTech Maritime, led by the EDA, offers a valuable forum for discussion on the development of defence systems.

To the extent that they enhance surveillance, in particular submarine capabilities, several projects within the Permanent Structured Cooperation (PESCO) and the EDA are relevant to strengthening cable resilience. These include the Maritime Unmanned Anti-Submarine System (MUSAS), ([101]) the Harbour & Maritime Surveillance and Protection (HARMSPRO) project ([102]) and the Maritime (semi-) Autonomous Systems for Mine Countermeasures (MAS MCM) ([103]). All of these initiatives aim at improving command and control capabilities, by developing new integrative platforms of multiple assets and sensors that can assist in countering threats to the cable network, as well as new mine-hunting capabilities.

([97]) Government of Portugal (2021), *Documentation of Seminar on Maritime Security. EUMC Mini Away Day*.

([98]) European Commission (2021), *Digital Day 2021: Europe to reinforce internet connectivity with global partners.*

([99]) European Union Institute for Security Studies (2021), *Naval Gazing? The Strategic Compass and the EU's Maritime Presence*.

([100]) European Defence Agency, *Maritime Surveillance (MARSUR)*.

([101]) Permanent Structured Cooperation, *Maritime Unmanned Anti-Submarine System (MUSAS)*.

([102]) Permanent Structured Cooperation, *Harbour and Maritime Surveillance and Protection (HARMSPRO)*.

([103]) Permanent Structured Cooperation, *Maritime (Semi-) Autonomous Systems for Mine Countermeasures (MAS MCM)*.

United Kingdom

As discussed in Section 4.3.1, the UK serves as a major link for the EU's digital connectivity with North America. Denmark is gaining importance as a strategic site, however, the UK will remain one of the most important nodal points in North Atlantic connectivity.

At present, there is no specific regulatory framework addressing submarine cable infrastructures or data connectivity in the UK, although cable security remains a common interest.

British security leadership has recurrently flagged cable protection as a top security issue. For instance, in January 2022, the Chief of Defence Staff warned that Russian submarine activity is threatening underwater cables. ([104]) He added that any damage to cables would be considered an act of war. ([105]) Multiple official documents reflect the UK's strategic focus on the issue. These include the 'Integrated Review of Security, Defence, Development and Foreign Policy' report, published by the British Parliament in 2021 , ([106]) and a refreshed of the National Strategy for Maritime Security (NSMS), to be published in 2025, which is expected to include an entire section on the issue. ([107])

In 2023, the UK acquired a new vessel, RFA Proteus, as part of its Multi-Role Ocean Surveillance Ship (MROSS) programme. RFA Proteus focuses on underwater surveillance and serves as a testbed to technologically advance the UK's Remotely Operated Vehicle (ROV) capabilities. ([108])The UK is also considering acquiring a second multi-role ocean surveillance vessel as part of its defence strategy. ([109]) However, as of the time of writing this report, the potential acquisition of a second vessel was under review, to ensure that its final specifications and intended role meet the UK's future strategic and defence needs. ([110])

2.3. North Atlantic Treaty Organization

Overview of actions taken by the North Atlantic Treaty Organization

The North Atlantic Treaty Organization (NATO) has long been aware of the vulnerabilities linked to critical submarine cable infrastructures across Member States. At the NATO Baltic Sea summit on 14 January 2025, leaders from across the region addressed the growing threat to critical submarine infrastructures. NATO's Secretary-General, Mark Rutte, underscored how recent sabotage had damaged energy and communication cables. He announced the deployment of new technologies, including a small fleet of naval drones, and highlighted that NATO will work with its Allies to integrate national surveillance assets, to improve the ability to protect critical submarine cable infrastructures and respond if required. NATO will work within the Critical Undersea Infrastructure Network, which includes industry, to explore further ways to protect

([104]) The Guardian (2022), *UK military chief warns of Russian threat to vital undersea cables*.

([105]) Kundaliya, D. (2022), *Russian harm to underwater cables could be 'act of war', UK defence chief warns*.

([106]) United Kingdom Parliament (2021), *UNCLOS: fit for purpose in the 21st century?*.

([107]) Bueger, C. and Edmunds, T. (2021), 'Innovation and New Strategic Choices. Refreshing the UK's National Strategy for Maritime Security', *The RUSI Journal*, 166(4), pp. 66–75.

([108]) European Security & Defence (2023), *UK's First Multi-Role Ocean Surveillance Ship Enters Service*.

([109]) Naval News (2023), *First of two MROS ships Arrives in the UK*.

([110]) UK Defence Journal (2025), *MoD tight-lipped on second undersea surveillance ship*.

infrastructure and improve the resilience of underwater assets. Executive Vice-President Henna Virkkunen participated in the summit, on behalf of the EU.

In parallel, in January 2025, NATO's Supreme Allied Commander General Christopher G. Cavoli launched the 'Baltic Sentry' mission to deter sabotage against critical submarine cable infrastructures in the Baltic Sea following several incidents of damage to cables. This initiative involves a range of assets, including frigates and maritime patrol aircraft. NATO relies on its Joint Force Command Norfolk for threat monitoring and the protection of submarine cable infrastructures. It also draws on its dedicated Maritime Centre for the Security of Critical Undersea Infrastructure (CUI), which supports the Commander of MARCOM in decision-making, force deployment and coordinated action. Additionally, NATO collaborates through the Critical Undersea Infrastructure Network, which includes industry partners, to explore new approaches to protecting infrastructure and enhancing the resilience of underwater assets.

EU–NATO partnership

The resilience of critical infrastructure is a shared concern for the EU and NATO. As such, a Task Force was set up in early 2023 to map out security challenges by focusing on the resilience of energy, transport, digital and space infrastructures. This work proved valuable for both organisations and resulted in a Final Assessment Report, published on 29 June 2023. ([111]) Under the umbrella of the EU–NATO structured dialogue on resilience, ongoing discussions have taken place between EU and NATO staff regarding critical maritime infrastructure, including submarine cables.

The issue of maritime infrastructure has also been central in the regular EU–NATO staff talks on maritime security. Most recently, in May 2025, EU and NATO staff participated in a scenario-based discussion on the protection of maritime infrastructure, facilitated by the Helsinki Centre of Excellence for Countering Hybrid Threats.

These exchanges serve as a valuable platform for sharing perspectives on common concerns and coordinating the implementation of respective tools and policies, such as the EU's Maritime Security Strategy and the EU Action Plan on Cable Security.

2.4. Overview of Member States regulatory and administrative frameworks

In 2024, the Commission issued a questionnaire to all 27 Member States to gain a better understanding of their legal and administrative frameworks to legislate, regulate, monitor and report submarine cable incidents. Member States were asked to provide information on a range of topics, including:

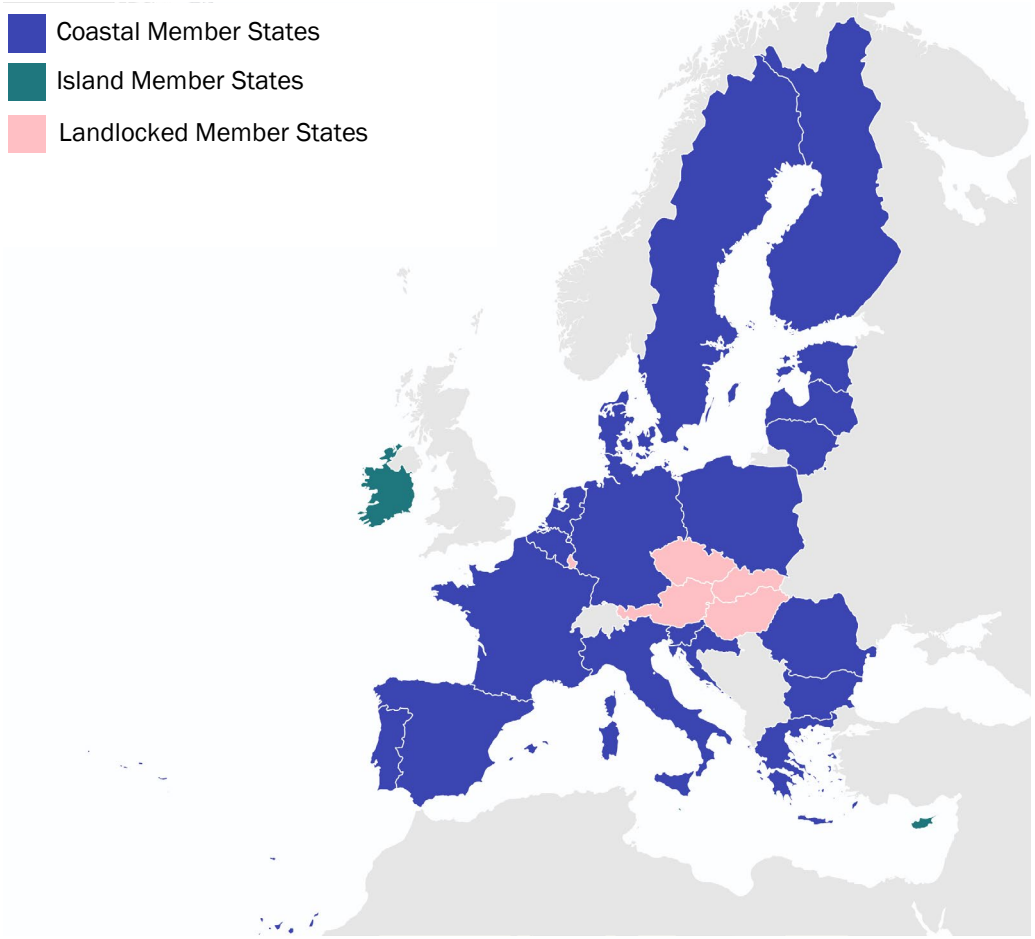
- status of submarine cable legislation
- preparedness against emergency situations and central reporting of submarine cable incidents
- national submarine cable authorities and collaboration between Member States and/or NATO.

Sixteen Member States submitted responses to the questionnaire, which are outlined below. It should be noted that the analysis presented below reflects the context at the time of the questionnaire responses in 2024, but the situation may have evolved in the meantime, in particular with the advancing transposition of the NIS2 and CER Directives.

([111]) NATO (2023), *NATO and European Union release final assessment report on resilience of critical infrastructure*.

In analysing the responses from Member States, one must consider that all Member States rely on submarine cable connections for their cross-continental internet traffic, but the level of dependence on submarine cables varies across Member States. Some are **island States** which rely exclusively on submarine cables for their connectivity (for example, Ireland, Malta and Cyprus), while a significant number of countries (Austria, Czechia, Hungary, Luxembourg and Slovakia) are **landlocked** and are heavily dependent on terrestrial connections and, consequently, are indirectly reliant on submarine cables provided by other Member States. Other Member States have a sea border (**coastal countries)** and host one or several submarine cable landing stations, increasing their reliance on submarine cables for their internet connectivity. These different categories are illustrated in Figure 2.3, below.

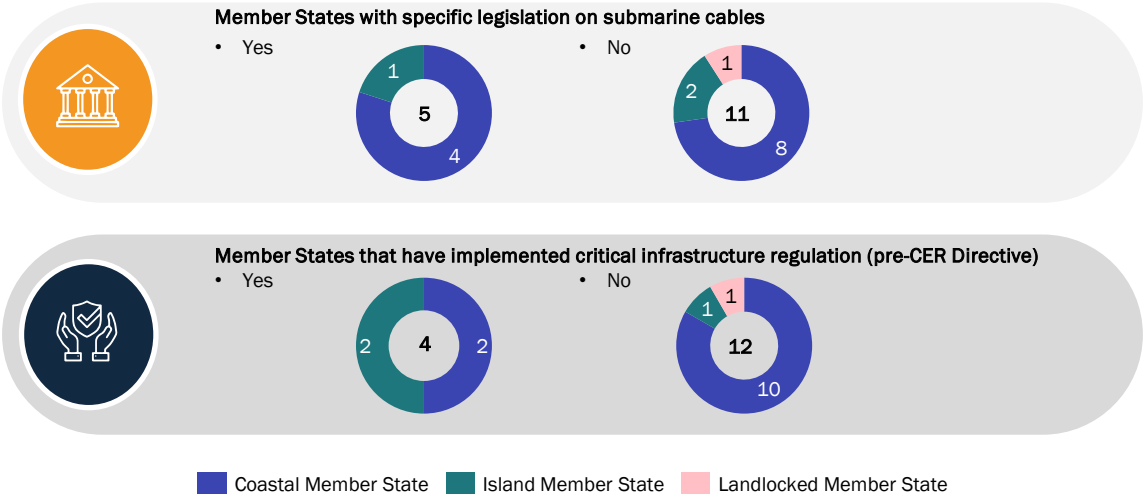
Figure 2.3: EU Member States, by category [Source: Analysys Mason, 2025]



2.4.1. Submarine cable legislation status

This section provides an overview of the current legislation on submarine cables in the 16 Member States, which replied to the Commission's questionnaire. Figure 2.4 summarises the main findings on legislation derived from the responses.

Figure 2.4: Summary of the main findings on legislation status across Member States [Source: Analysys Mason, 2025]



Submarine cable legislation across Member States

Overall, the majority of Member States that replied to the questionnaire do not have submarine cable-specific legislation in place. Typically, submarine cables are part of legislation with a wider scope, for example, Telecommunications Acts, general building or construction permits, maritime safety requirements or environmental regulations. Only five Member States have legislation specifically governing submarine cables, four of which are coastal Member States and one is an island Member State. Where such legislation is in place, it typically covers matters related to the resilience of physical infrastructure, including cables, landing stations and beach manholes, as well as cybersecurity. In one case, the legislation specifies the penalties applicable for damaging submarine cables, and requires that any damage be reported to the nearest port within 24 hours, while failure to comply may result in monetary penalties and potential imprisonment for responsible parties.

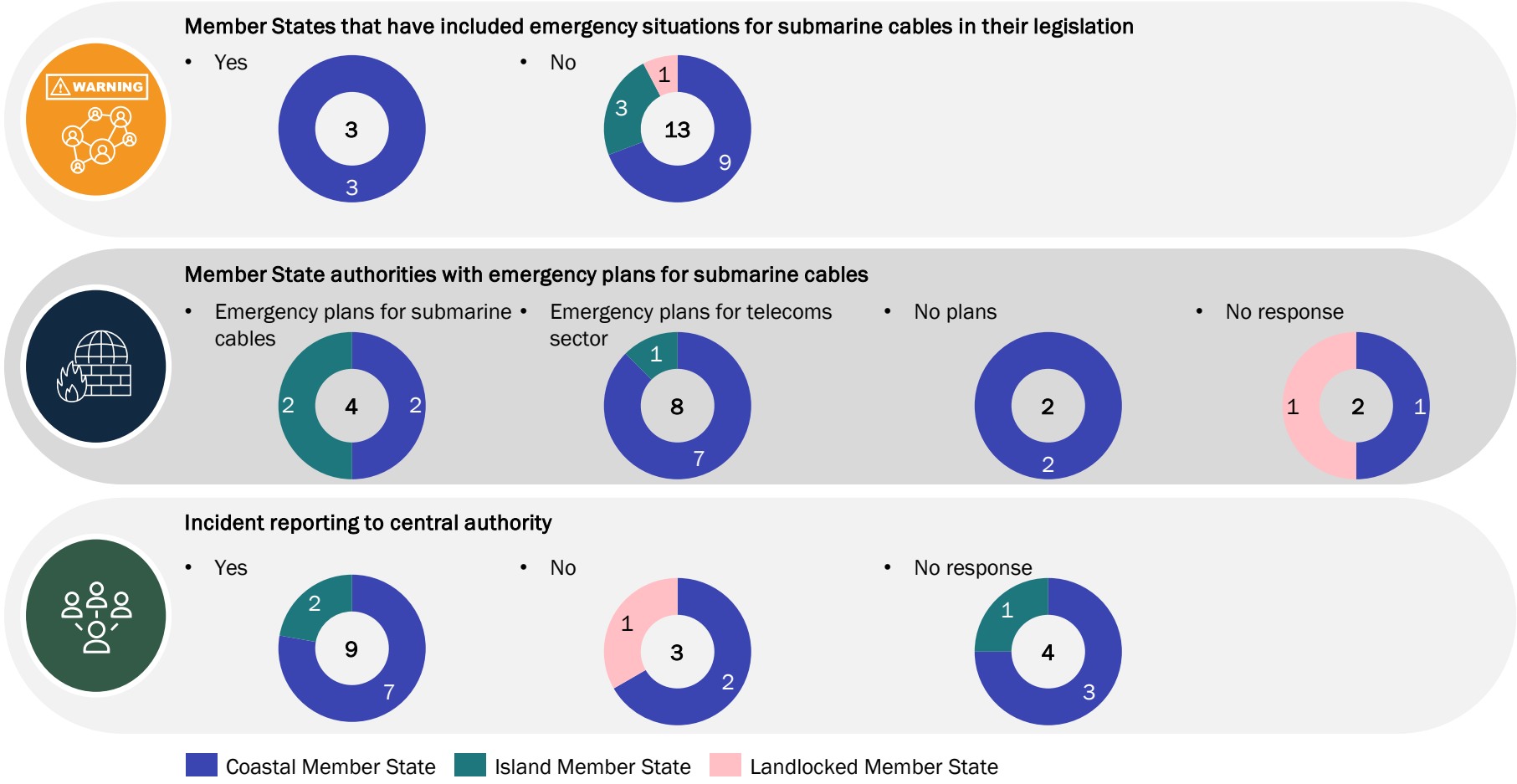
Implementation of critical infrastructure regulation

Four out of the 16 Member States that responded to the Commission's questionnaire had implemented critical infrastructure regulation into State laws before the EU issued the CER Directive, as shown in Figure 2.4. Two are island Member States and the other two are coastal Member States.

2.4.2. Preparedness against emergency situations and reporting of incidents

This section provides an overview of the extent to which Member States and authorities with existing emergency plans incorporate emergency situations into their legislative frameworks, based on the 16 responses received from Member States. A summary of the main findings is provided in Figure 2.5, below.

Figure 2.5: Summary of the main findings on emergency plans [Source: Analysys Mason, 2025]



Inclusion of emergency situations in the legislation

As shown in the above figure, three coastal Member States have legislated for emergency situations related to submarine cables. The legislation aims to ensure that all relevant State authorities – including those responsible for submarine cables – remain operational and are capable of safeguarding the population during emergencies.

Provision of a submarine cable emergency plan by the relevant authority

It should be noted that these emergency plans are not mandated by legislation but are instead developed by the relevant authorities and, as a result, the outcomes differ from those described in the previous subsection.

Four Member States (two coastal countries and two island nations) indicated that they have emergency plans specific to submarine cables in place. These emergency plans outline measures to ensure the continuation of essential communication services in the event of a disruption, such as use of alternative routes. Eight Member States (one island nation and seven coastal countries) stated that they have overarching emergency plans for the telecoms sector, encompassing provisions related to submarine cables. Two Member States indicated that they do not currently have any emergency plan in place, while the remaining two states did not provide a response.

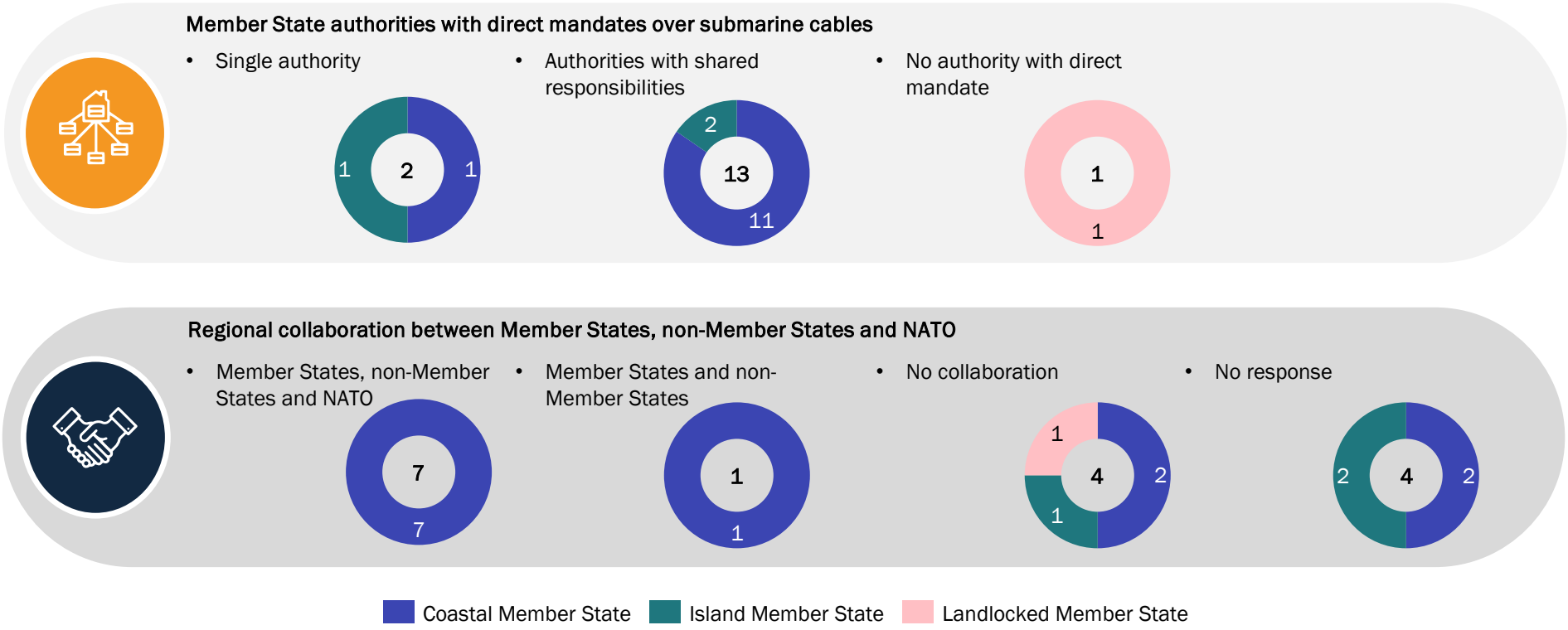
Provision of a central authority for incident reporting

Nine Member States (seven coastal countries and two island nations) indicated that they have a central authority to which submarine cable incidents are reported. Three Member States (two coastal countries and one landlocked country) stated they have no central authority for incident reporting. The remaining four Member States did not provide a response specific to incident reporting.

2.4.3. National submarine cable authorities and collaboration between Member States and/or NATO

This section provides an overview of existing administrative structures across Member States, based on the 16 responses received to the Commission's questionnaire. A summary of the main findings is provided in Figure 2.6 below.

Figure 2.6: Summary of Member State authorities with mandates over submarine cables and emergency situations [Source: Analysys Mason, 2025]



Authorities with direct mandates for submarine cables

Two Member States (one coastal nation and one island nation) reported the existence of a central authority empowered to directly coordinate responses to submarine cable incidents across all relevant authorities.

Thirteen Member States (11 coastal and 2 island countries) indicated that multiple authorities shared the responsibility over submarine cables, each holding mandates over specific areas (such as licensing and permits, monitoring and reporting, physical security and cybersecurity). The remaining Member State (a landlocked country) reported that there was no authority with direct responsibility for coordinating issues that may affect submarine cables.

Inter-State coordination and/or coordination with NATO

Member States indicated varying levels of coordination with other Member States, non-EU countries and organisations such as NATO and the North Sea Joint Declaration. Eight Member States (all coastal countries) reported that one or more authorities within their jurisdiction are members of, or collaborate with, NATO and other Member States on matters related to submarine cable security and resilience. ([112]) Additionally, four Member States (two coastal nations, one island country and one landlocked State) indicated that they do not collaborate with other Member States or NATO in relation to submarine cable resilience. The remaining Member States (four) did not provide a response.

As an example of direct cooperation between Member States, in April 2024, six North Sea countries (Belgium, Denmark, Germany, the Netherlands, Norway and the UK) pledged to improve information and knowledge sharing to better protect critical submarine infrastructure from foreign interference and disruption. ([113]) Furthermore, it should be noted that the EU Action Plan on Cable Security, presented in Section 2.2.2, promotes cooperation between Member States to support the development of a surveillance mechanism for submarine cables and a dedicated regional hub using the Baltics as a test bed.

This may be supported by a non-public Memorandum of Understanding on the Protection of Critical Undersea Infrastructure in the Baltic Sea, signed between the EU, eight Member States as well as Norway and Iceland in Vihula, Estonia, at the Ministerial Session of the Council of the Baltic Sea States on 16 May 2025.

2.4.4. G7 and beyond

During a United Nations General Assembly event on 25 September 2024, the EU endorsed the New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World, together with key partners (i.e., the US, the UK, Canada, South Korea, Japan, Singapore, Australia and New Zealand). ([114]) It lays out principles to ensure submarine cable infrastructures are secure, reliable, sustainable and resilient. The principles include

([112]) Of these, three Member States collaborate with both other Member States and NATO, while one Member State collaborates solely with other Member States.

([113]) Government of Norway (2024), *Six North Sea Countries Join Forces to Secure Critical Infrastructure*.

([114]) European Commission (2024), *Commission welcomes Joint Statement on the security and resilience of undersea cables at UN General Assembly in New York*.

recommendations to select low-risk submarine cable providers, follow cybersecurity best practices, enhance route diversity and protect cable networks from unauthorised access to data in transit.

On 14 March 2025, the Foreign Ministers of Canada, France, Germany, Italy, Japan, the UK and the US issued a declaration, ([115]) reaffirming their commitment to a secure and open maritime domain. The declaration highlights the critical role of maritime security in global stability and economic resilience, addressing threats such as strategic contestation, illicit shipping activities and disruptions to maritime routes. It underscores the importance of UNCLOS as the legal framework for maritime governance. The declaration also addresses the importance of submarine cables, highlighting that 97% of global data flows through them, making submarine cables vital for international communication and economic stability.

The G7 Foreign Ministers also underscore the importance of developing regional security initiatives, protecting critical maritime infrastructure and combating maritime crime. They express concern over the growing risks to the security of submarine cables, through sabotage and unintentional damage, which can lead to internet disruptions and delays in data transmissions. The G7 Foreign Ministers emphasise the need for enhanced co-operation between Member States to ensure the resilience of submarine infrastructure, maritime supply chains and the protection of freedom of navigation and overflight. The G7 welcome the Cable Action Plan described in Section 2.2.2 of this report.

This declaration follows the earlier joint statement ([116]) on the security and resilience of submarine cables issued by the G7 Foreign Ministers in November 2024, emphasising the critical importance of submarine cables. The statement highlighted the unparalleled capacity and reliability of these cables. It reflected similar sentiments around the resilience of submarine cables and called for enhanced cooperation between governments, advocating for best practices in cybersecurity, spatial planning and risk management. The statement also encouraged transparent ownership and governance structures for cable providers and stressed the importance of complying with international and domestic laws to protect submarine cables.

Several European governments have also taken steps to strengthen public–private partnerships regarding submarine cables. For instance, following the damage of the Balticconnector gas pipeline between Estonia and Finland in 2023, the Norwegian government co-operated with its energy companies to first map oil and gas pipelines and then the electrical grid and submarine data cables. ([117])

([115]) United States Department of State (2025), *G7 Foreign Ministers Declaration on Maritime Security and Prosperity*.

([116]) UK Department for Science, Innovation & Technology (2024), *New York joint statement on the security and resilience of undersea cables in a globally digitalized world*.

([117]) Detsch and Johnson (2024), *NATO Wants to Boost Its Undersea Defenses*; and S&P Global (2023), *Norway's Gassco Keeps Eye on Security Situation After Balticconnector Damage*.

3. THE TELECOMS SUBMARINE CABLE MARKET, VALUE CHAIN AND ECOSYSTEM

There are almost 600 active optical submarine cables around the world, of which 200 have at least one landing station in an EU Member State. ([118]) Approximately 97–98% of the global internet traffic transits through submarine cables. ([119]) Although the dependence on submarine cables in Europe is slightly reduced compared to the rest of the world due to the significant terrestrial network between European countries, it is crucial to have a resilient submarine cable infrastructure and a strong ecosystem to purchase, supply and maintain optical submarine cables.

3.1. Definition of routes and regions

Throughout this report, we differentiate between submarine cable routes that connect Member States to external countries and routes that interconnect Member States together (intra-Member State connectivity routes). For each of these two types of routes, we consider up to five regions, as explained below.

Connectivity routes between Member States and non-EU countries

Member States are connected to non-EU countries through submarine cable routes which can be categorised into five different geographical regions:

- **North Atlantic** – all submarine cables connecting Member States to North America (transatlantic)
- **Red Sea and Indian Ocean** – all submarine cables connecting Member States to Asia through the Red Sea and to countries in the India Ocean, including countries located on the East coast of Africa
- **South Atlantic** – all submarine cables connecting Member States to the West coast of Africa and South America
- **Mediterranean** – all submarine cables connecting Member States to non-EU countries in the Mediterranean Sea, including North African countries, Egypt, Israel and Türkiye
- **Northern Europe** – all submarine cables connecting Member States to non-EU countries in the Baltic Sea, North Sea, Irish Sea and English Channel, including the UK and Norway.

Intra-Member State connectivity routes ([120])

Member States are connected together through submarine cable routes which can be categorised into four different geographical regions:

- **North Atlantic** – all submarine cables interconnecting Member States in the North Atlantic region, including those between mainland Portugal and the Azores, as well as between the Azores and the Madeira Islands
- **South Atlantic** – all submarine cables connecting mainland Spain and the Canary Islands and interconnecting the Canary Islands together

([118]) Analysys Mason (2025), Submarine cable database 1H 2025.

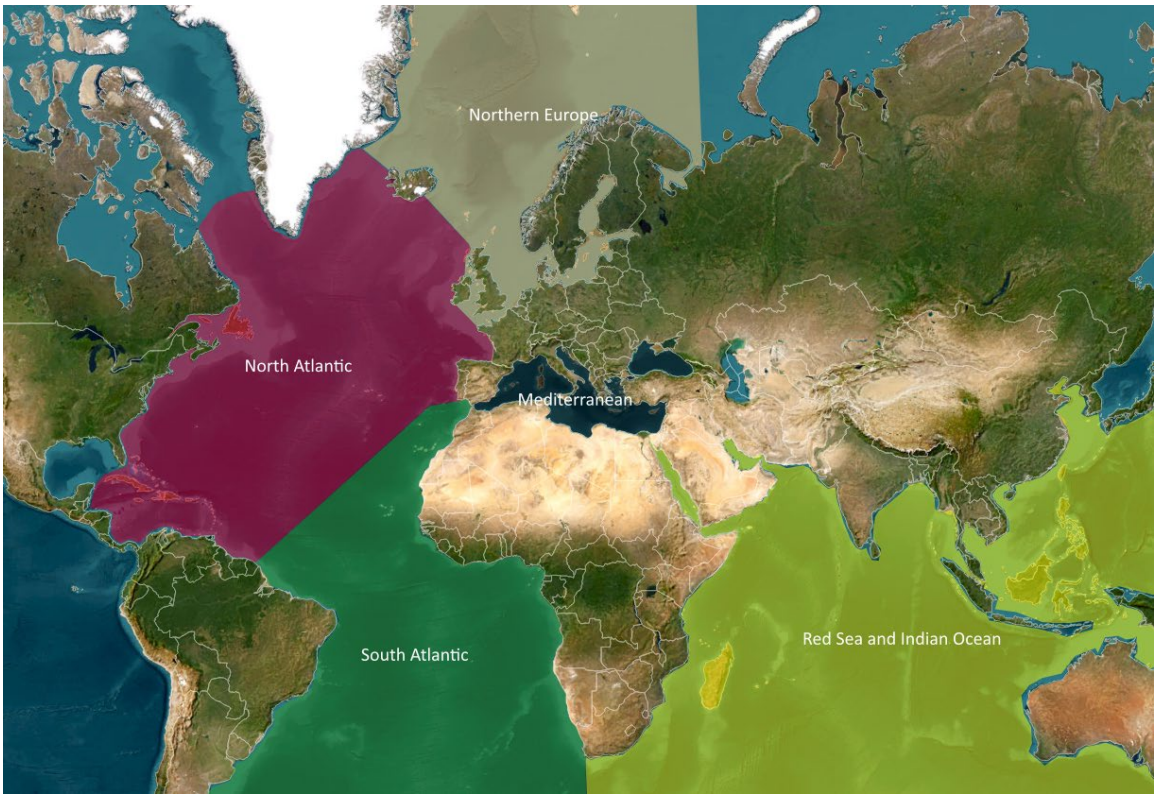
([119]) European Commission (2024), *Subsea telecommunication cables are essential for Europe's digital connectivity.*

([120]) Submarine cables considered in intra-Member States connectivity routes also encompass routes to the outermost regions of Member States (for example, cables connecting the Canary Islands to mainland Spain).

- **Mediterranean** – all submarine cables connecting Member States in the Mediterranean Sea
- **Northern Europe** – all submarine cables interconnecting Member States in the North Sea and Baltic Sea region.

These regions are illustrated in Figure 3.1, below.

Figure 3.1: Regions defined for route analysis [Source: Analysys Mason, 2025]



3.2. Key stakeholders in the submarine cable market

The submarine cable ecosystem is characterised by five groups of stakeholders:

- submarine cable owners and investors
- submarine cable suppliers
- providers of submarine cable components
- submarine cable installation and maintenance providers
- submarine cable project consultancy and engineering companies.

Each of these groups is discussed in turn below.

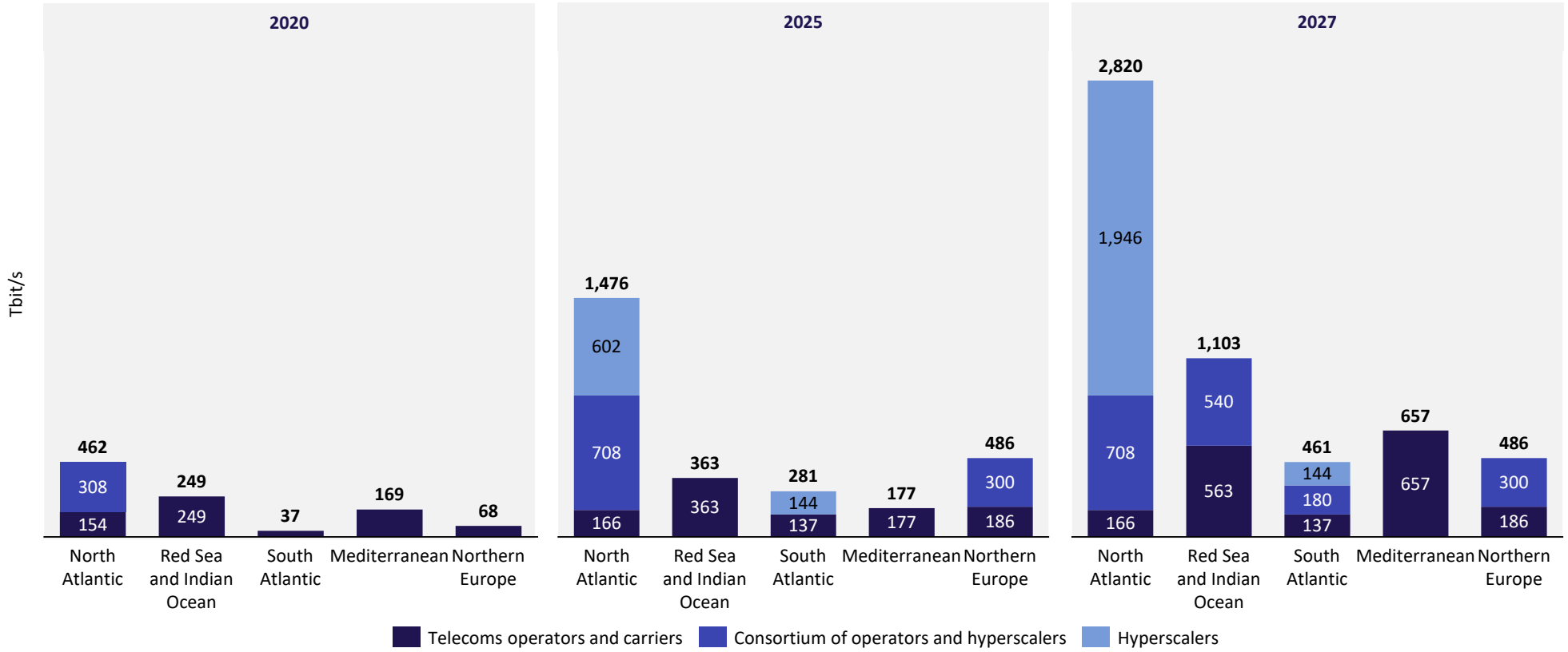
3.2.1. Submarine cable owners and investors

Until the mid-1990s, cable owners consisted of monopolistic or dominant telecoms operators, often government-backed incumbents such as BT (UK), AT&T (US), Telecom Italia (Italy), Telefónica (Spain) and France Telecom (now Orange, France). These submarine cable owners were fully vertically integrated and often invested collaboratively in submarine cables. By the turn of the century, independent private cable owners such as Global Crossing started to appear on the market as a consequence of telecoms deregulation. They also formed consortia with historical operators.

From 2005, hyperscalers such as Google Cloud Infrastructure ('Google'), a subsidiary of Alphabet, and Meta (Facebook) started to lease an increasing amount of managed capacity from different cable consortia. The continued growth of traffic prompted hyperscalers to rethink their international connectivity strategy and, in 2010, Google started investing in submarine cables as part of a consortium with the Unity cable, connecting Chikura (Japan) to Los Angeles (US). Following a few investments in submarine cable consortia, hyperscalers started to invest in private cables in 2018. In 2019, as part of a consortium, Google invested in its first European submarine cable known as Havfrue, connecting the US to Ireland and Denmark, with a total capacity of 108 Tbit/s.

Figure 3.2 provides the evolution of capacity ownership for the different regions connected to the EU.

Figure 3.2: Evolution of capacity ownership per region connecting Member States to non-EU countries [Source: Analysys Mason, 2025]



- **North Atlantic –** As of January 2025, 89% of the transatlantic cable capacity was owned by hyperscalers such as Google and Meta (either solely or as part of a consortium), which currently dominate the transatlantic capacity supply market in Europe. ([121]) This is primarily driven by the need to interconnect the US and European regional clouds, which requires a significant amount of bandwidth (i.e., data-centre-to-data-centre interconnection). This capacity dominance will be further increased by 2027, with hyperscalers projected to own up to 94% of the North Atlantic capacity.

- **Red Sea and Indian Ocean –** In comparison, the current capacity in the Red Sea, which interconnects the EU to the Middle East and Asia, is solely owned by traditional telecoms operators, where Chinese operators such as China Unicom, China Mobile and China Telecom, as well as Chinese holdings such as the Hentong Group (owners of HMNTech) are well represented. Other operators owning capacity on this route include Singtel (Singapore), Reliance Jio (India), Telecom Egypt, Pakistan Telecom, e& (formerly Etisalat, UAE), Orange and Djibouti Telecom, among others. However, the current deployment of large-capacity cables ([122]) by hyperscalers in this region will more than double the current capacity along the Europe-to-Asia route by 2027. This reflects the growing volume of cloud regions deployed by hyperscalers in the Middle East and Asia.

- **South Atlantic –** Similarly to the Red Sea and Indian Ocean region, up until 2023, the submarine cable capacity along the Western Africa route was fully owned by historical operators such as Telkom, Orange, Angola Telecom, Telecom Namibia and Portugal Telecom (currently Altice Portugal), as well as international operators such as AT&T and Deutsche Telecom. However, the launch of Google's Equiano cable in 2023 means that, at the time of writing this report, half of the capacity on the South Atlantic route is owned by Google. Furthermore, with the deployment of 2Africa by a consortium led by Meta, hyperscalers will own approximately 70% of the capacity either through private cables or as part of a consortium.

- **Mediterranea Sea –** Given the more regional nature of the Mediterranean Sea, traditional telecoms operators and carriers such as Orange (France), Cyta (Cyprus), Algeria Telecom (Algeria), Turk Telecom (Türkiye), Bezeq Telecom (Israel), Telecom Egypt (Egypt), Ooredoo (Qatar) and Telecom Italia (Sparkle, Italy) own the infrastructure in different consortia, and no hyperscaler is part of any of these consortia. It should be noted that, with the deployment of the Medusa submarine cable, Orange and AFR-IX Telecom will own 75% of the total capacity in the Mediterranean Sea. It is also important to note that submarine cable systems traversing the Mediterranean Sea to join the Red Sea are accounted for as part of the Red Sea and Indian Ocean route.

- **Northern Europe –** As of January 2025, a consortium composed of Meta, Aqua Comms (US) and Bulk Fiber Networks (Norway) owned 62% of the capacity delivered to Northern Europe via the 300 Tbit/s Havhingsten submarine cable connecting Denmark, the UK and Ireland. The remaining capacity in that region was owned by more traditional operators and carriers such as BT (UK), Sure (UK), Vodafone (UK), Tata Communications (India), Virgin Media Business (UK), eir (Ireland), EirGrid (Ireland), TDC (Denmark), Tele2 (Sweden) and Global Connect (Denmark), among others.

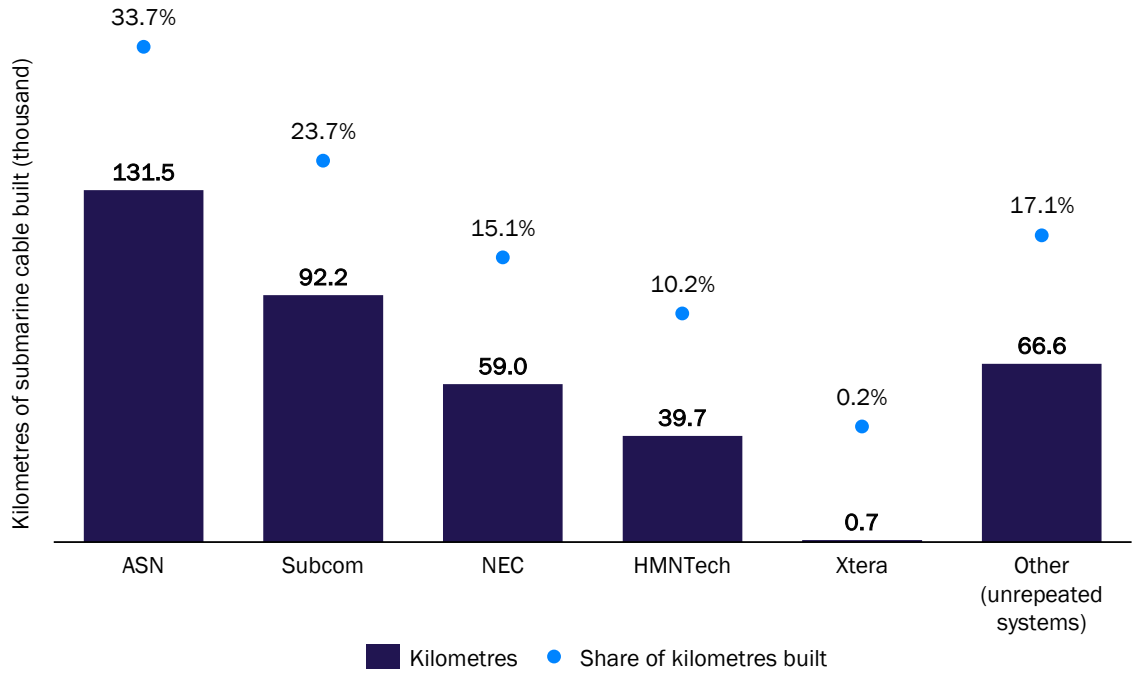
[121] As part of the multi-fibre submarine cable deployed by hyperscalers, some fibres are swapped with historical operators (for example, Orange) in exchange for fibre pairs located in different geographies and different routes.

([122]) Blue-Raman (built by Google and Telecom Italia Sparkle), India-Europe-Xpress (IEX) (owned by Meta, China Mobile and Reliance) and South East Asia-Middle East-West Europe 6 (SMW6, owned by a consortium including Microsoft, Singtel and Bangladesh Submarine Cable Company).

3.2.2. Submarine cable suppliers

The global submarine cable market is dominated by four Tier 1 system suppliers: European Alcatel Submarine Networks (**ASN**), headquartered in France, **Subcom** (US), Nippon Electric Company (**NEC**, Japan), and **HMNTech** (formerly called Huawei Marine Networks, China). Based on the distance of submarine cable deployed between 2020 and 2024, the four main players combined hold an estimated market share of approximately 83% of total submarine cable length deployed, with ASN being the lead supplier (with around 34% market share) and HMTech being a distant fourth player with approximately 10% of the market. ([123]) XTera is another submarine cable supplier but has different capabilities compared to the aforementioned suppliers, as it does not manufacture its own submarine cables. The remaining 17% market share is owned by smaller suppliers providing short (unrepeated) submarine cable systems and with limited capabilities. The relative market share of submarine cable suppliers is illustrated in Figure 3.3.

Figure 3.3: Market share of the main global submarine cable suppliers – length of cable deployed between 2020 and 2024 [Source: Submarine Telecoms Forum, 2024]



All four submarine cable suppliers also maintain strong ties with their respective governments and financial institutions:

- the French government acquired 80% of ASN in 2024, and ASN is supported by European financial institutions (the European Investment Bank (EIB) and CEF)
- Subcom has strong ties with the US Department of Defense to provide non-commercial systems, and secured a USD 10 million-a-year contract in 2021 from the US Department of Transportation (DOT) to run a two-vessel fleet to provide submarine cable security ([124])

([123]) Submarine Telecoms Forum (2025), *Industry Report 2024-2025*.

([124]) Marine Technology News (2023), *Inside the Subsea Cable Firm Secretly Helping America Take on China*.

- NEC is financed by Japanese banks, including the Japan Bank for International Cooperation (JBIC); in light of recent developments in the submarine cable market, the Japanese government has announced that it will increase its support for NEC, recognising the strategic importance of submarine cables following incidents of suspected sabotage targeting these infrastructures in Northern Europe and Taiwan ([125])([126])
- HMNTech is owned by the largest power and fibre-optic cable manufacturer in China.

([125]) The Asahi Shimbun (2025), *Japan fighting uphill battle in protecting web of undersea cables*.

([126]) Agenzia Nova (2025), *Japanese government to fund submarine cable installation for national security reasons*.

Figure 3.4: Overview of the four main suppliers of submarine cable systems worldwide [Source: Analysys Mason, Europacable 2025]

Supplier	ALCATEL SUBMARINE NETWORKS	SUBCOM	NEC	HMN TECH
Ownership and funding	• Owned by the Agence des participations de l'État (APE), which is owned by the French government (80% stake) and Nokia (20% stake) • Supported by EU funding and financing (the EIB and CEF)	• Owned by Cerberus Capital Management, a US private equity firm • Close to the US Department of Defense (provides non-commercial systems)	• Public company largely owned and funded by Japanese banks and the Japan Bank for International Cooperation (JBIC)	• Owned by Hengtong Group (81%), ([127]) the largest power and fibre-optic cable manufacturer in China • The remaining 19% is owned by New Saxon (UK) • Huawei fully divested its shares in 2020 from Hengtong Group
Submarine system capabilities	• Fully integrated turnkey submarine network solutions	• Partially integrated turnkey submarine network solutions • Manufactures cables, wet equipment and uses Ciena transponders	• Partially integrated turnkey submarine network solutions • Provides cables, wet and dry equipment	• Partially integrated turnkey submarine network solutions • Manufactures cables, wet equipment and uses Huawei transponders
Installation and maintenance capabilities	• Owns four installation and three maintenance vessels with a global presence	• Owns eight installation vessels, including two formerly used as maintenance vessels • Main client is Google	• No maintenance or installation capabilities; outsources these activities to third parties	• No maintenance or installation capabilities, outsources to Global Marine and other providers
Market share ([128]) (2020–2024)	• 34%	• 24%	• 15%	• 10%
Annual manufacturing capacity (km)	• >50 000	• >50 000	• >40 000	• ~20 000

([127]) Hengtong Group is a private company owned by institutional investors and individual shareholders and has established a Communist Party branch to reflect its alignment with Chinese government principles.

([128]) Based on the length of submarine cable installed. Source: Submarine Telecoms Forum, 2024.

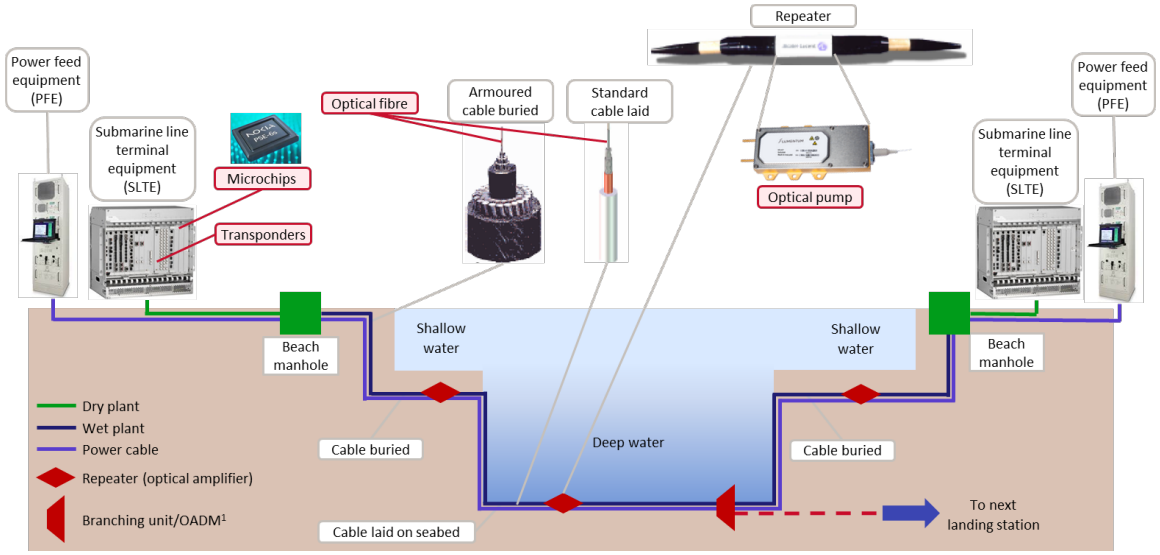
3.2.3. Providers of submarine cable components

Submarine system suppliers purchase key components from a small number of companies, which creates key dependencies in the supply chain. The main submarine cable components include:

- optical fibre
- cables
- repeaters
- branching units and Reconfigurable Optical Add-Drop Multiplexers (ROADM)
- Power Feed Equipment (PFE)
- submarine line termination equipment (SLTE) and transponders
- Distributed Acoustic Sensing (DAS) systems
- microchip and other components.

Figure 3.5 below illustrates the different components of a submarine cable system.

Figure 3.5: Configuration of a submarine cable system [Source: Analysys Mason, 2025]



The supply chain for each of the above components is examined below.

Optical fibre

Optical fibre is a key component of submarine cable systems as it is required to transmit high-capacity data along long distances. The technology for data transmission has evolved significantly since the first cable was deployed, from a single wavelength over Single-Mode Fibre (SMF) with 0.001 Tbit/s capacity, to modern-day optical fibres that transmit tens of terabits per second (Tbit/s) of data per fibre pair, with low signal loss (bolstered by repeaters). ([129]) Modern submarine systems use multiple fibre pairs ([130]) in the same cable to further increase capacity to several hundreds of Tbit/s.

([129]) Sumitomo Electric Technical Review (2023), *Optical Fibres for High Fibre Count Submarine Cable Systems.*

([130]) Using Space Division Multiplexing (SDM) technology, modern submarine systems are deployed with either 8 (for example, Marea), 10 (for example, SMW6), 12 (for example, Dunant and FA-1), 16 (for example, Grace Hopper and Amitie) or 24 (for example, Anjana) fibre pairs.

The design of submarine optical fibres differs from that of terrestrial optical fibres because the conditions under which they operate differ significantly. Also, given the distance involved, submarine optical fibres are designed with an ultra-low attenuation (i.e., low loss) compared to terrestrial systems. Only three companies currently manufacture submarine optical fibres for repeated (i.e., long-distance) submarine cable systems globally, which creates a dependency for the EU. These companies are:

- Corning Incorporated (US)
- Optical Fiber Solutions (OFS, formerly Lucent Technologies, US)
- Sumitomo Electric (Japan).

European optical fibre manufacturers include Nexans (France) and Prysmian/Norddeutsche Seekabelwerke (NSW, Germany). However, these companies typically produce optical fibre for terrestrial applications and the characteristic of these fibres is not appropriate ([131]) for ultra-long-distance submarine cable applications. Therefore, optical fibre from European manufacturers can only be used for relatively short submarine cable systems.

Cables

Once the optical fibre is manufactured, it has to be enclosed in a protective casing to ensure its durability. The four leading submarine cable system suppliers (ASN, Subcom, NEC and HMNTech) each manufacture their own cables. Each of the main suppliers has a specialised department to manufacture both armoured and non-armoured cables, to ensure they withstand the high moisture and pressure in the high seas, as well as fish net tugging and seaquakes. Xtera subcontracts its cable to companies such as Nexans (France) and Prysmian/NSW (Germany).

Repeaters

The repeater provides the optical amplification for the signal to compensate signal attenuation as it travels through the optical fibre. Submarine cable systems equipped with repeaters are usually referred to as **repeated systems**, and those with no repeaters are usually referred to as **unrepeated systems**. Repeaters are usually required every 80 km to 100 km, except in unrepeated systems, which are typically less than 250 km. ([132]) The main suppliers all manufacture their own repeaters, using third-party components.

A key third-party component for repeaters is the semiconductor optical pump, which provides the necessary amplification to the optical signal. Erbium-Doped Fibre Amplifiers (EDFA) use a rare element, erbium, which emits a wavelength of light that amplifies the optical signal from the fibre. Lumentum (US) and Coherent Corp (US) are the only suppliers of high-reliability pumps suitable for submarine cables, ([133]) and each organisation has a single manufacturing plant, one in the US and one in Switzerland, for submarine class laser pumps.

Optical pumps therefore create a significant dependency in the supply chain for all submarine cable system suppliers.

([131]) Corning, OFS and Sumitomo can all produce ultra-low-loss optical fibre (i.e., with a loss lower than 0.16 dB/km), which cannot currently be emulated by any European optical fibre manufacturer.

([132]) The length of a repeated submarine cable system can range between 250 km to tens of thousands of km.

([133]) There are providers of optical pumps for terrestrial systems (for example, 3SP Technologies (France)) which are less reliable than the pumps produced by Lumentum and Coherent Corp, and therefore not suitable for submarine cable systems.

Branching units and reconfigurable optical add-drop multiplexers

The branching unit is a junction point that splits the fibre into two directions, one of these directions being the local landing station and the other being the continuation of the cable. Optical Add-Drop Multiplexers (OADMs) are used to selectively add or drop specific wavelengths of light from an optical fibre without affecting the other channels. The OADM is typically located in a separate device from the branching unit. In modern cable systems, OADMs are dynamically reconfigurable to change the wavelengths that can be dropped at a particular landing station.

ASN, NEC and Subcom manufacture their own ROADMs on their submarine cable systems, using some components from third parties.

Power feeding equipment

The Power Feeding Equipment (PFE) is the terminal equipment in the landing station which powers the repeaters to ensure the signal can be amplified along the submarine cable system. It comprises a mid-voltage transformer with an output voltage of up to 18 kV. PFE is designed to be highly reliable, incorporating redundant systems to ensure continued supply in the event of a component failure, and has multiple safety features such as discharge protection, emergency power-off and alarms for unusual voltage. The current propagates along the conductive section located around the optical fibre, and the outer circumference of the conductive material is covered with isolation such as polyethylene.

ASN and NEC typically assemble their own PFE, ([134]) while Subcom and Xtera outsource to Spellman High Voltage Electronics (US), and HMNTech outsources to Powerland (China).

Transponders and submarine line terminal equipment

Transponders convert (modulate) electrical signals into the optical signals that transmit data in the optical fibres. They also demodulate the optical signals into electrical signals at the receiving end. Each transponder connected to the same fibre uses a different colour of light (wavelength), which means that multiple transponders can transmit in parallel in the same fibre without interfering with each other. This principle is called Wavelength-Division Multiplexing (WDM). Modern transponders provide bandwidth of up to 800 Gbit/s. A core part of the transponder is the Digital Signal Processor (DSP), which is a programmable, real-time processor of optical signals, and the Application-Specific Integrated Circuit (ASIC), which is used for data processing and signal conversion.

As of 2025, up to 40 wavelengths can be multiplexed and transmitted concurrently in the same fibre pair, providing a total bandwidth of 20–30 Tbit/s. In Space Division Multiplexing (SDM) cables, up to 24 fibre pairs can be provided in the cable, delivering a total bandwidth of up to 500 Tbit/s. ([135])

Transponders are hosted in the SLTE. The latter also typically hosts the WDM multiplexers and demultiplexers, which enable several wavelengths to be multiplexed together in the same fibre pair. Historically, SLTE and transponders were only provided by the turnkey submarine cable suppliers, and the upgrade to the cable capacity was conducted by the same supplier, adding transponders in the existing SLTE. Therefore, ASN and NEC manufacture their own SLTE and transponders, while

([134]) However, they procure individual components from third-party providers.

([135]) The state-of-the-art 24-fibre-pair cable Anjana has a total capacity of 480 Tbit/s (i.e., 20 Tbit/s per fibre pair).

Subcom and HMNTech rely on Ciena and Huawei, respectively, to supply their transponders. ASN provides the same DSP as its former owner Nokia, but with enhanced features, and uses a third-party DSP from Acacia, which is now part of Cisco. NEC uses DSPs from NEL, a subsidiary of NTT.

Historically, submarine cable suppliers also provided line terminal equipment and associated transponders, which are the active transmitting devices on submarine cables. However, with the advent of the ITU open cable standard (ITU G.977), cable owners can now install transponders from a different vendor than the one that supplied the submarine cable system (for example, ASN, HMNTech, NEC and Subcom). Implementation of the open cable standard has led to a dramatic reduction in the price of transponders, as the transponder market has opened up to more traditional terrestrial optical transmission system vendors such as:

- Ciena (largely owned by Fidelity Management and Research Company and the Vanguard Group)
- Nokia (Finland)
- Infinera (acquired by Nokia in February 2025)
- Huawei (China).

Distributed Acoustic Sensing systems and Science Monitoring and Reliable Telecommunications nodes

Various sensing technologies can be integrated into submarine cables, including optical techniques such as Distributed Acoustic Sensing (DAS) and Science Monitoring and Reliable Telecommunications (SMART) cables, which embed physical sensors into newly deployed wet infrastructure. This subsection provides a detailed overview of DAS systems, SMART nodes and their associated ecosystems. ([136])

Distributed Acoustic Sensing systems

An increasingly important technology in the submarine cable industry is Distributed Acoustic Sensing (DAS), which uses the optical fibre optic to detect and measure acoustic signals along the length of the cable. In DAS systems, the optical fibre itself acts as the sensing element to detect any mechanical disturbance near the cable which could be created by a nearby ship, an ROV on the seabed or by natural movement of the seabed (undersea seismic activity, volcanos, landslides, etc).

DAS is quite a mature technology, as it has been used for many years in terrestrial applications such as pipeline integrity monitoring in the oil and gas industry, ([137]) or for traffic control and track integrity monitoring in the railway industry. ([138])

Since DAS systems operate by sending a signal in the fibre and listening to the echo coming back, the range of DAS systems in submarine applications is limited to the distance to the first repeater, which is usually 80–100 km. For unrepeated systems (i.e., short systems with no repeaters), the range of DAS systems can be up to 200 km. DAS systems can be implemented using either a dedicated fibre or the same fibre as the one used for optical transmission. ([139]) In the latter case, DAS systems can be retrofitted on existing submarine cables, as no special fibre or additional

([136]) Other sensor technology includes State of Polarisation (SoP) but is less used and not discussed in this report.

([137]) Pimentel Niño, M.A., (2017), *DAS: Pipeline Monitoring and the Blue Colour of the Sky*, ILF Consulting Engineers.

([138]) Laemmerhirt A., Schubert M., Drapp B., Zeilinger R (2022), *Fiber Optic Sensing for Railways - Ready to Use?*.

([139]) But using a different set of wavelengths (i.e., using a wavelength in the L-Band spectrum).

equipment is required to be fitted along the submarine cable and the only additional equipment required is located at the landing station.

The benefit of equipping submarine cables with DAS systems is that vessels or ROVs close to a submarine cable equipped with this technology could be detected. Combining Automatic Identification Systems ([140]) (AISs) and DAS technology could ultimately enable to define the unique signature of vessels and ROVs so that, if these vessels/vehicles come close to submarine cable systems without their AIS, they could be recognised due to their unique signature. However, the signal processing technology required to perform this functionality is still nascent and is not commercially available at the time of writing this report.

As of 2025, only a few submarine cable systems are known to be equipped with DAS. Among European submarine cable systems, Tampnet ([141]) (connecting Northern Europe) and EllaLink ([142]) (connecting Brazil, Portugal and Morrocco) have both publicly announced the use of DAS technology. There might be other European submarine cable systems equipped with DAS, but this information has not been disclosed publicly.

There are several DAS system providers including Luna Innovations (US), FiberSense (Australia), ([143]) FEBUS (France) and DSIT (Israel). More recently, ASN has developed a DAS solution for its own submarine cables. ([144])

It should also be noted that DAS systems can detect the movement of submarine vessels. As a result, the cable infrastructure could be considered as a 'legitimate' military target in the case of a war scenario, which further highlights the need for several redundant cable routes to prevent service outage.

Science Monitoring and Reliable Telecommunications nodes

A Science Monitoring and Reliable Telecommunications (SMART) node integrates environmental sensors (for example, temperature, pressure, seismic acceleration) into submarine optic cables. These enhanced cables offer a dual function: reliable telecoms and continuous environmental monitoring. Their applications include:

- climate change observation, including ocean circulation and sea-level trends
- tsunami and earthquake early warning, supporting disaster risk reduction
- seismic activity monitoring, aiding research into the Earth's structure and geohazards
- risk assessment, informing sustainable development of coastal and offshore infrastructure
- hazard detection, helping to identify external threats to cable integrity and improving routing strategies.

Pilot projects are already underway, such as the SMART Atlantic CAM ring system, which will connect mainland Portugal, the Azores and Madeira. Several companies are involved in the development and deployment of SMART cables, including ASN, Prysmian and Subcom.

([140]) AIS is a short-range coastal tracking system currently used on vessels. It was developed to provide identification and positioning information to both vessels and shore stations.

([141]) Bjørnstad, S. (2022), *Using the fibre cables as sensors, detecting security threats and earthquakes*, Tampnet AS.

([142]) EllaLink (2020), *EllaLink & EMACOM launch the "EllaLink GeoLab" SMART submarine cable initiative*.

([143]) FiberSense (2022), *FiberSense and SX announce expansion of alliance with deployment of monitoring and protection capability on new NEXT submarine cable between AUS, NZ, USA and the Pacific Islands*.

([144]) ASN, *OPTODAS The leading technology for distributed acoustic sensing*.

Furthermore, it should be noted that SMART nodes need to be part of the original design of the submarine cable, as they cannot be retrofitted. Additionally, SMART nodes can only detect movement or vibration within a certain radius, and therefore do not provide the continuous sensor system along the fibre cable as DAS systems.

Microchip and other components.

Finally, all electronics components for terminal equipment depend upon the availability of state-of-the-art microchips. Microchips used in SLTE for transponders use 3 nanometre (nm) and 5 nm microchip technology (i.e., spacing between transistors on the chip). At the time of writing, Ciena is the only transponder vendor using state-of-the-art 3 nm microchip technology for its Wavelogic 6 transponders ([145]), giving Ciena an advantage over its competitors in terms of power consumption and bandwidth. It is also understood that Infinera/Nokia and NEC are developing a 3 nm microchip for their next-generation transponders.

However, at present, only two companies are capable of manufacturing 3 nm microchips: Taiwan Semiconductor Manufacturing Corporation (TSMC, Taiwan) and Samsung (South Korea). Nokia and Ciena design their own transponder microchips and use both TSMC and Samsung foundries to manufacture them. This creates a significant dependency on TSMC and Samsung, as no other companies can provide these advanced manufacturing services. Given the interest in Taiwan by the Chinese government, TSMC has started to diversify the location of its production by building advanced manufacturing plants in the US, Japan and in Germany (Dresden), which was facilitated by large subsidies from these governments ([146]) – the EUR 10 billion manufacturing plant in Dresden is planned to start production in late 2027 –. ([147]) These plans are aligned with the EU European Chips Act, adopted in 2023, which aims at doubling Europe's share of global semiconductor production by 2030. In addition, it should be noted that Dutch company ASML has recently developed a technology (i.e., computational lithography) which enables the production of nanometre microchips at scale. ([148])

Historically, Huawei has used TSMC for manufacturing its transponder microchips. However, since November 2024, the US government has imposed export restrictions to TSMC, preventing it from providing advanced manufacturing services (i.e., 7 nm microchips and more advanced nodes, such as 3 nm microchips) to Chinese companies. ([149]) This export restriction on TSMC was then extended to Samsung in January 2025. ([150]) Therefore, Huawei is now using Semiconductor Manufacturing International Corporation (SMIC, China) as its microchip manufacturer; at the time of writing this report, however, SMIC was not yet equipped to manufacture the latest generation of microchips (i.e., 3 nm technology).

([145]) Ciena (2025), *Ciena Unveils WaveLogic 6, Industry's First 1.6Tb/s Coherent Optic Solution*.

([146]) The Japan News (2025), *TSMC to Launch Full-Scale Production in Japan, U.S., Germany as Part of 'Silicon Shield' Against China*.

([147]) Global Finance (2024), *TSMC Starts Building Its First European Chip Plant*.

([148]) ASML (2025), *Changing the world, one nanometer at a time*.

([149]) Reuters (2024), *US ordered TSMC to halt shipments to China of chips used in AI applications*.

([150]) The Korea Times (2025), *US regulations on China-bound chips to weigh on Samsung Electronics*.

3.2.4. Submarine cable installation and maintenance providers

Historically, some submarine cable suppliers (for example, Subcom) were also the ones installing and maintaining these cables; however, not all suppliers had this capability. Consequently, some international carriers such as Orange, BT, C&W, AT&T, Singtel, e& (formerly Etisalat), NTT and KDDI invested in maintenance vessels to maintain their own cables, as operating laying vessels was a complementary business for operators. The growing deployment of submarine cables in the early 2000s also led to the emergence of some independent installation and maintenance suppliers, such as Optic Marine Services (OMS).

As of 2025, there are 53 vessels capable of installing and/or maintaining **repeated telecoms submarine cables** worldwide, including 24 cable-laying vessels and 29 cable-repair vessels, as shown in Figure 3.6 below. ([151])

([151]) Annex B and Annex C provide detailed information on installation and maintenance vessels, respectively.

Figure 3.6: Submarine cable installation and maintenance suppliers worldwide [Source: Analysys Mason, 2025

Vessel owners	Ownership	Cable laying vessels	Maintenance vessels	Total vessels
Subcom	Ceberus Capital Management (US)	8	–	**8**
ASN	80% French government, 20% Nokia (Finland)	4	3	**7**
GMSL	Keppel Infrastructure Fund (Singapore)	2	4	**6**
OMS	Private (Malaysia), KKR (US)	1	4	**5**
E-Marine	e& (formerly Etisalat) (UAE)	1	3	**4**
Orange Marine	Orange Group (France)	1	3	**4**
Elettra	Orange Group (France)	1	1	**2**
S.B. Submarine System	Joint venture between China Telecom and GMSL (China and Singapore)	3	–	**3**
Kokusai Cable Ship (KCS)	KDDI Group (Japan)	1	2	**3**
NTT	NTT Group (Japan)	1	2	**3**
Asean Cableship (ACPL)	Singtel as majority shareholder (Singapore)	–	2	**2**
FiberHome	FiberHome Telecommunication Technologies (China)	1	–	**1**
IT International Telecom	Privately owned (Canada)	–	1	**1**
LS Marine Solution	67% LS Cable and System, 6% KT Corporation	–	1	**1**
Limin Marine & Offshore	Privately owned family business (Indonesia)	–	1	**1**
Bina Nusantara Perkasa (BNP)	Privately owned (Indonesia)	–	1	**1**
Jala Nusantara Mardika	Sarana Global Indonesia (Indonesia)	–	1	**1**
Total		**24**	**29**	**53**

In addition, there are hybrid multipurpose vessels which are used in small basins for the repair and installation of small power cables and small unrepeated telecoms submarine cables. Examples of multipurpose vessel owners are provided in Figure 3.7 below, while further details are presented in Appendix D. Please refer to Section 3.4 for a comparison of the different types of vessels.

Figure 3.7: Examples of hybrid vessel owners for the maintenance of small/unrepeated submarine cables [Source: Analysys Mason, 2025]

Vessel owners	Ownership	Total multipurpose vessels
Baltic Offshore	Sweden	2
Lilaco	Finland	1
Seaworks	Norway	1
Total		**4**

It should be noted that the list of vessels contained in this report differs from the list of vessels provided by the International Cable Protection Committee (ICPC), for a number of reasons. First, the ICPC list omitted 11 vessels from several owners including ASN, Orange Marine and Subcom. Second, the ICPC list includes the Raymond Croze, a vessel which was decommissioned in 2024. Lastly, the ICPC list includes barges, tugboats and vessels used for the installation of submarine cables in shallow waters, which have restricted use and functionalities.

A list of 23 vessels – comprising 15 vessels with limited use and functionalities originally included in the ICPC list, 4 multipurpose vessels (as identified in Figure 3.7) and 4 multipurpose vessels from JD Contractors A/S – is provided in Appendix D. ([152]) Further, it is worth noting that the ICPC is not responsible for managing the list of vessels, but the responsibility for updating fleet information lies with each ICPC member.

Regarding submarine cable maintenance, this is organised into geographical zones. There are three types of maintenance agreements:

- **Club maintenance agreements**, in which cable owners collaborate and share a pool of maintenance resources (vessels and crews from several maintenance suppliers) and where the costs are transparently shared between them.
- **Private maintenance agreements**, in which cable owners share a pool of maintenance resources (vessels and crews from several maintenance suppliers) but where the maintenance suppliers negotiate a commercial price and service level agreements (SLA) with each cable owner separately.

Regional private agreements, where cable owners have a direct contract with a single maintenance provider (typically with multipurpose maintenance companies, as illustrated in Figure 3.7)

Not all maintenance vessels reflected in Figure 3.6 are used in the maintenance agreements, as some are reserved for use locally due to cabotage laws, for example.

([152]) Source: Axiom, ICPC.

3.2.5. Submarine cable project consultancy and engineering companies

In the submarine telecoms industry, project and engineering consultancy companies play a crucial role for submarine cable buyers with limited engineering or project management capabilities, as they provide the required skills for ensuring the smooth design, planning and compliance of cable systems as well as their smooth installation.

In the submarine telecoms industry, there are two key consulting skills:

- **Optical systems engineering** – includes the expertise on the design of the submarine cable, assignment of wavelengths within the optical fibre(s) and expertise of all active equipment (including PFE, SLTE, transponders, repeaters, branching units and DAS systems) required to build a submarine cable system.
- **Marine consultancy** – includes the expertise related to all the marine services required to install the system along an appropriate route (including cable route desktop study, marine seabed survey, seabed clearance, cable lay and burial), both for planning the cable and onboard vessels.

A small number of specialised consultancy firms can provide both optical system expertise and marine expertise, including, but not limited to:

- Aqest (France) ([153])
- Axiom (France)
- DRG Undersea Consulting (US)
- Pioneer Consulting (US)
- Subsea Networks (UK). ([153])

There are also a few companies solely specialised in marine consultancy services such as Ocean Cable Consultants (Italy), Red Penguin Marine (UK) and Pelagian (UK), which mainly provide onboard representation of the cable owner.

There are also a number of independent submarine expert individuals, who can either work as subcontractors with large, general consultancy companies, or as individuals with cable owners that have specific requirements.

In addition, it is worth noting that many carriers such as Orange or Telecom Italia have retained in-house expertise and do not typically use project consultancy and engineering companies. Although hyperscalers, such as Meta and Google, have built significant engineering, marine and project management expertise within their own teams, they sometimes require the assistance of external consultancy companies to complement their teams, given the large scale of their submarine cable projects.

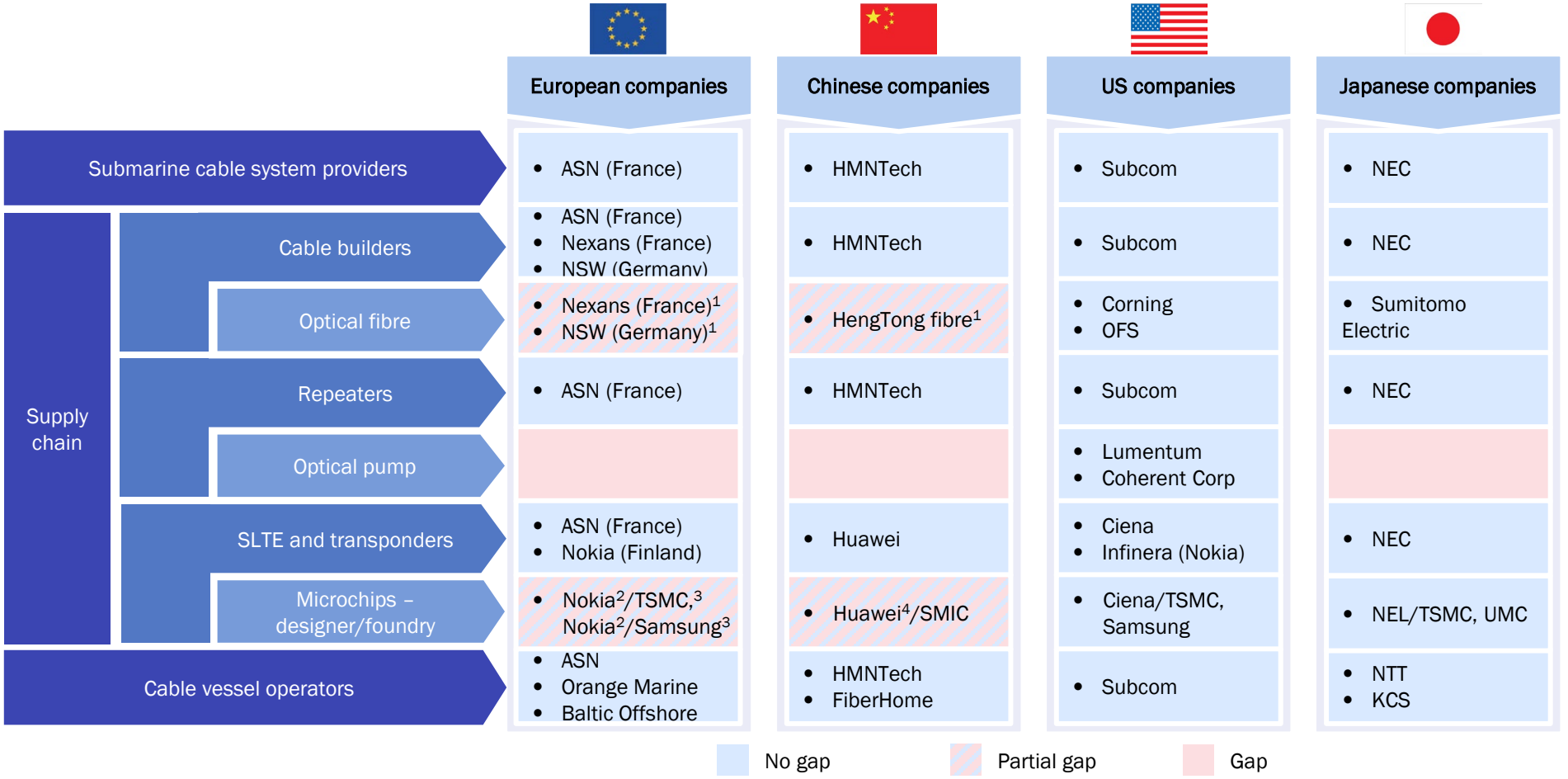
Overall, the scarcity of companies offering submarine cable project and engineering consultancy services poses a challenge, especially for cable owners with limited technical knowledge.

3.2.6. Summary

Figure 3.8 provides a summary of key stakeholders in the submarine cable ecosystem and identifies gaps in the supply chain.

([153]) Only two to three staff.

Figure 3.8: Key players and EU supplier dependencies in the submarine cable ecosystem ([154]) [Source: Analysys Mason/Axiom, 2024]



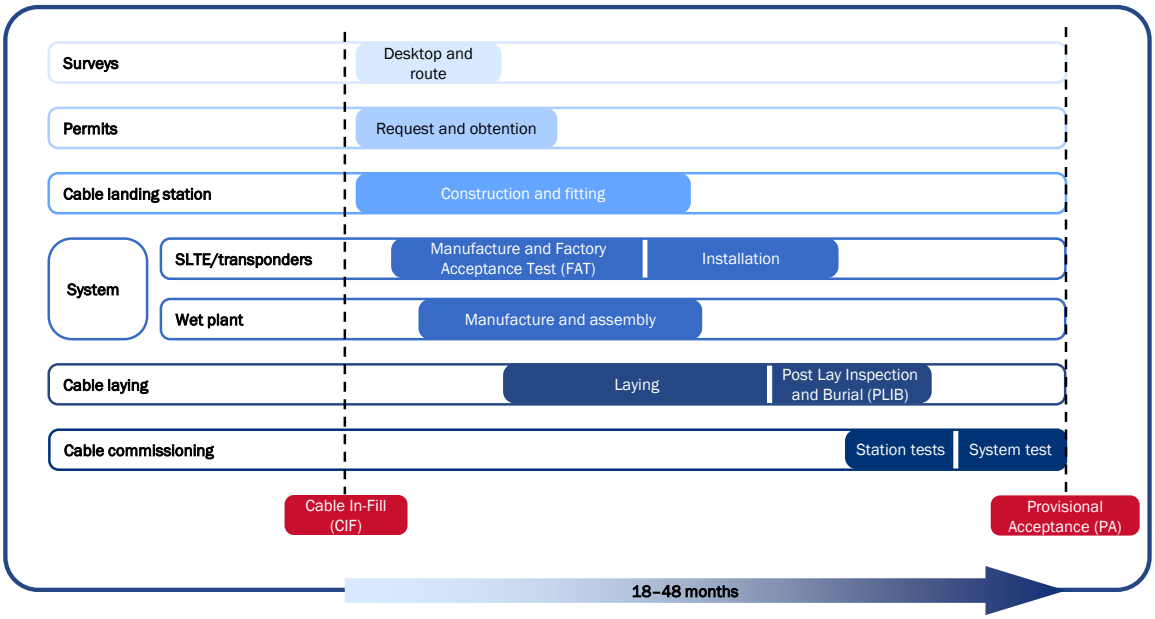
([154]) (1) Only for small unrepeated submarine systems; (2) Lack of state-of-the-art European foundry, although TSMC is building a new plant in Germany to mitigate Chinese take-over threat; (3) TSMC (Taiwan, under US influence) and Samsung (South Korea); (4) The US is preventing TSMC from providing microchips to Huawei, hence Huawei uses SMIC, which has volume-production issues.

3.3. Installation, maintenance and repairs

3.3.1. Submarine cable installation

Figure 3.9 outlines the various stages involved in the implementation of a submarine cable project, which are described in turn below.

Figure 3.9: Submarine cable implementation tasks and timelines [Source: Analysys Mason, 2025]



Surveys (desktop and route)

Once the supply contract for the design, manufacture, installation and commissioning of the system has been signed, the first step is to select and define the route. The decision criteria to select a route include the cable type or armouring that will be needed in some locations, the extent to which the cable will need to be buried, and the avoidance of protected zones and conflict areas.

The definition of the route consists of two steps: a desktop survey followed by a route survey. During the desktop survey, the system supplier gathers all available information on the areas where cable is planned to be installed (study of underwater depth of ocean floors (bathymetry), sea current, weather forecast, fishing, etc.) to define a preliminary route, which is then submitted to the owner for review. If accepted, the preliminary cable route is then physically surveyed by a vessel, using various electronic devices, including a multi-beam echo sounder and a side-scan sonar, to create an image of the sea floor. This image is then used to assess burial feasibility where plough burial is required.

The optimum cable route is usually a compromise between the need to reduce the risks for the system and the cost of additional protection (longer route, more armour, increased burial).

Permits (request and obtention)

Several permits and authorisations are required for the implementation of a submarine cable system. Permits are usually divided into two categories:

- **Operational permits** – these include all necessary permits to perform the work, such as the survey, installation, custom clearance and visas. Such permits fall under the responsibility of the contractor.
- **Permits in principle** – these are the necessary permits and authorisations to operate and maintain a submarine cable system in a specific country and includes the authorisation to use or lease the beach, the seabed portion where the cable will be installed and the relevant telecoms licences. In theory, obtaining the permits falls under the responsibility of the cable owners, specifically the relevant landing party responsible for operating and maintaining the infrastructure. In some cases, for example, when crossing a third-party territory, the contractor is required to make all necessary demands on behalf of the owner. Typically, the permit in principle requires an environmental impact assessment, including sometimes a specific survey, to demonstrate that the cable route and the landing selected will minimise impacts on various areas such as wildlife, coral, archaeological sites, fishing or sanding dredging zones.

Each country defines its own set of required permits and granting procedures. This often results in a permitting process that is long, complex and unpredictable, and requires exchanges with several administrations, also in the official local language.

Cable landing station (construction and fitting)

Usually, the landing station already exists, and only limited work is required to make it fit for purpose (for example, refitting a transmission room or upgrading the power plant). However, in some cases, the landing station needs to be constructed, which is a complex undertaking as it has to be designed to mitigate system outages (for example, it has to cope with a grid outage by providing own power through generators and Uninterruptible Power Supply (UPS), which provide near-instantaneous protection by switching to energy stored).

One way to mitigate the issues associated with the complexity of building a landing station is to use modular containers, which are delivered with pre-equipped electrical wiring and equipment. Individual container modules can be assembled on site. In such cases, the landing party only has to provide the necessary land, concrete slab and the connexions to basic utilities, significantly reducing the time required to have the landing station ready for service.

System (manufacture and installation)

As discussed in Section 3.2.3, a submarine cable system requires a large number of elements (for example, fibre cable, repeaters, branching units, SLTE and transponders) to be manufactured and then assembled together. For example, the optical fibre needs to be produced to specifications, as standard fibres cannot be used for such complex systems. Considering the high ability and reliability required by the system, the various steps of the manufacturing process – from product design to the Factory Acceptance Test (FAT) – are carefully monitored by the inspection authority designated by the owner/consortium.

Cable laying

When the system is ready, it can be delivered at the depot, from where it can be loaded onto the tank of the selected installation vessel. The choice of the specific installation vessel is important, as it has to have the right tools to avoid installation issues. For example, if the cable needs to be buried in shallow water at a particular depth, it is important that the vessel has a plough which supports this type of trenching.

The vessel then instals the cable along the selected route by either burying the cable (typically in shallow water) or just laying the cable on the seabed (typically in high seas where human activity such as fishing or anchoring cannot reach).

Once the system has been buried, the Post Lay Inspection and Burial (PLIB) is carried out in order to check that the cable has been buried according to the initial specifications. This phase usually relies on ROVs to both inspect and improve burial/protection (for instance, water jetting to bury the cable into the seabed or placing rocks on it).

Cable commissioning

Once the system is installed and connected to landing stations, it needs to be commissioned. This operation consists of 'turning on' the system and making all the necessary tests to confirm that the system operates as planned, including both station and system tests.

Acceptance

System acceptance, also known as Provisional Acceptance (PA), occurs at the end of the successful commissioning test period, when final payments are made to the system supplier and the ownership is transferred to the project promoter consortium (together with the operational risk).

3.3.2. Submarine cable maintenance and repair

In case of service disturbance or operational failure, submarine cable maintenance typically involves six main steps to ensure the cable remains functional and any issues are promptly addressed. These steps are:

- fault identification and location
- operational permit request
- preparation of spares and cables
- transit to the fault location
- repair of fault
- transit back to base.

Each of these steps is described briefly below.

Fault identification and location

The first step is to identify the type of fault and the location of the fault. This is usually achieved by the Network Operations Centre (NOC) monitoring the submarine cable. The NOC needs to identify if the fault is due to a faulty component (for example, a faulty repeater), a cable break or another reason. The location of the fault needs to be identified to ensure that the vessel stops at the exact location of the repair.

In the case of a fibre break, the location of the fault is usually identified using an Optical Time Domain Reflectometer (OTDR). This device sends a signal through the fibre and measures the time it takes for the signal echo to return to the point of origin.

Sometimes, faults can be very complex to diagnose, either because there are multiple causes for the fault or because the fault cannot be located precisely (for example, a shunt fault where the cable may have been crushed and the earth is in contact with a phase conductor).

Operational permit request

Most faults occur within territorial waters or EEZs, and only rarely in international waters. As a result, the maintenance provider typically needs to request an operational permit to access the affected area once the fault has been identified and intervention in the wet plant is required. Operational permits do not usually constitute a bottleneck in the repair process, especially in Europe, as they can be obtained within a few days. This is in marked contrast with permits in principle, which can take several months or years to secure, as discussed in Section 3.3.1. The request for an operational permit is usually made immediately after diagnosing the fault, with the objective to obtain approval just before the repair vessel arrives at the fault location.

Preparation of spares and cable

Once the fault has been identified and located, the necessary repair equipment and spares are loaded from the vessel owner's depots where all spares are stored. The spares required at the depot include fibre cable, repeaters and branching units, as well as power electrical feed equipment ([155]) from the submarine cable provider. It is important to ensure that spares are available at the depot, as ordering equipment from different suppliers can cause further delays in the repair process. It should be noted that spares are usually specific to each systems.

Transit to the fault location

Once all spares are loaded and the specialist crew is on board, the vessel can depart from its base and travel to the fault location. The depart time/day depends on weather conditions. The transit travel speed is usually between 12 and 15 knots (between 22 km/hour and 28 km/hour) in good weather. When bad weather is forecast, the vessel may need to stop before reaching the repair site and anchor until the weather improves.

Repair of fault

Assuming the fault is located between two specific locations (location A and location B), the repair process involves the following steps:

- cut the existing cable in location A using a grapple or a remotely operated underwater vehicle
- bring up the existing cable end in location A to the surface and attach to a buoy
- cut the cable in location B using a grapnel or an ROV
- bring up the existing cable end in location B and connect with the replacement cable by splicing the fibres and installing a joint unit to protect the spliced fibres
- recover the A end of the cable and splice it to the other end of the replacement cable
- perform OTDR tests to ensure the quality of the splicing is adequate

([155]) PFE is only needed for repeated submarine cables.

- if the test is successful, the entire fibre is put back to the seabed
- if in shallow water, a new trench is required to be made by a burial machine to bury the cable.

Transit back to base

Finally, the vessel needs to transit back to base from the fault location, requiring a time that must be considered as part of the maintenance process.

3.3.3. Maintenance agreements

Maintenance companies have fleets of repair vessels strategically located to provide the quickest response to requests from cable owners and operators, and are available 24/7 on a standby basis. As described in Section 3.2.4 of this report, there are currently three types of maintenance agreements:

- club maintenance agreements (see Figure 3.10)
- private maintenance agreements (see Figure 3.11)
- regional private agreements (for example, Baltic offshore, which provides commercial services in the Baltics).

Each type of agreement is organised into geographical zones and can coexist especially where there is a high density of submarine cables. It must be noted that not all suppliers and vessels are part of a maintenance agreement as, for example, some maintenance companies and associated vessels are exclusively used nationally (for example, Indonesia), where cabotage laws are enforced.

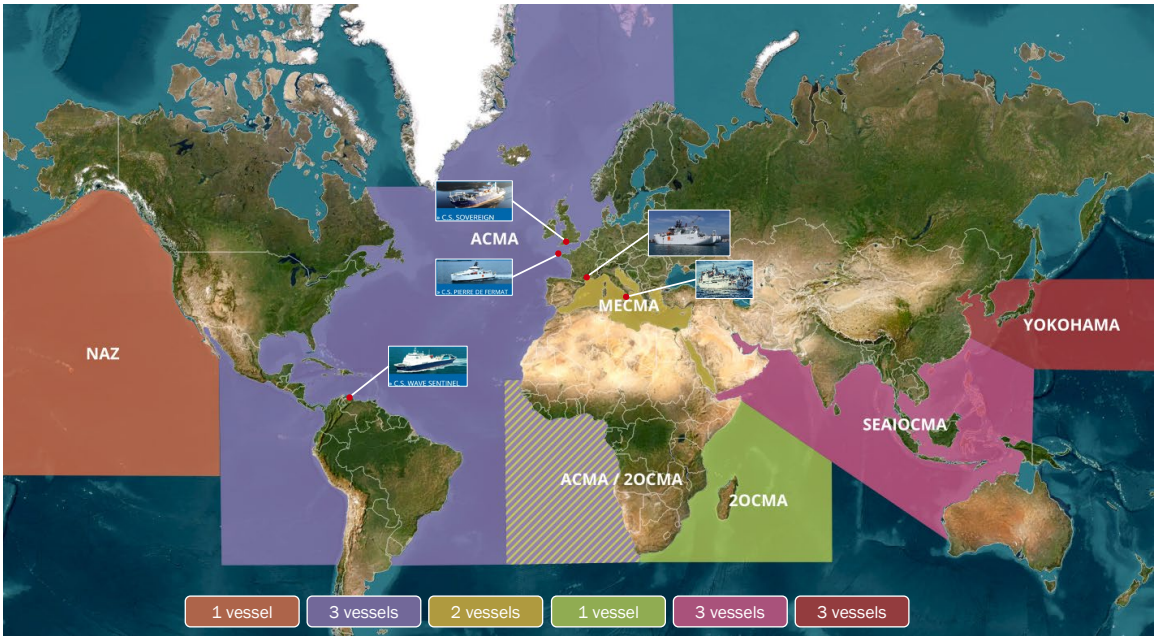
Club maintenance agreements

In this type of agreement, the beneficiaries of submarine cable maintenance services in a particular region come together to create a not-for-profit consortium, where the maintenance costs incurred are shared transparently between cable owners based on the length of submarine cable that each owner possesses. Club maintenance agreements typically involve several maintenance suppliers in each geographical region.

There are six major club maintenance agreements established globally for the maintenance of submarine cables, as illustrated in Figure 3.10 below:

- the Atlantic Cable Maintenance and Repair Agreement (ACMA)
- the Mediterranean Cable Maintenance Agreement (MECMA)
- the 2 Oceans Cable Maintenance Agreement (2OCMA)
- the South East Asia and Indian Oceans Cable Maintenance Agreement (SEAIOCMA)
- the Yokohama Zone Cable Maintenance Agreement, and
- the North American Zone Cable Maintenance Agreement (NAZ).

Figure 3.10: Club maintenance agreements [Source: Analysys Mason, 2025]



Each of these agreements is described in turn below:

- **ACMA** – this is one of the largest club maintenance agreements, with 57 members including power cable and oil & gas companies. It covers the Atlantic, the North Sea, the Baltic Sea and West Africa, and is therefore a key maintenance agreement for European submarine cables. ACMA relies on three dedicated maintenance vessels based in Brest (France) operated by Orange Marine, in Curaçao, operated by Global Marine, and in Portland (UK), also operated by Global Marine.
- **MECMA** – this agreement covers the Mediterranean Sea, the Black Sea and the Red Sea, and is therefore also crucial for the maintenance of European submarine cables. MECMA currently has 40 members, including members with domestic cables connecting the mainland to islands. MECMA relies on two dedicated maintenance vessels, one based in La Seyne-Sur-Mer (France), operated by Orange Marine, and one based in Catania (Italy), operated by Elettra.
- **2OCMA** – this agreement covers the southern Atlantic and Indian Oceans, and relies on Orange Marine as its main maintenance provider, which operates a dedicated vessel based in Cape Town (South Africa).
- **NAZ** – this agreement spans from Alaska to the Equator and covers both coasts of North and South America. Global Marine (Singapore) oversees the operations from its base in Victoria (Canada), with a single vessel.
- **SEAIOCMA** – this agreement covers an extensive area from Djibouti (Africa) to Guam (North Pacific Ocean). Maintenance is carried out by three dedicated vessels based in Singapore, Sri Lanka and Subic Bay (the Philippines), from two maintenance providers: ACPL (Singapore) and Global Marine (Singapore).
- **Yokohama** – this agreement focuses on the northern Asia and northwest Pacific regions, and relies on three main maintenance providers (KCS (Japan), LS Marine Solution (South Korea) and SBSS (China and Singapore), which operate three dedicated vessels based in Yokohama (Japan, Geoje (South Korea) and Wujing (China).

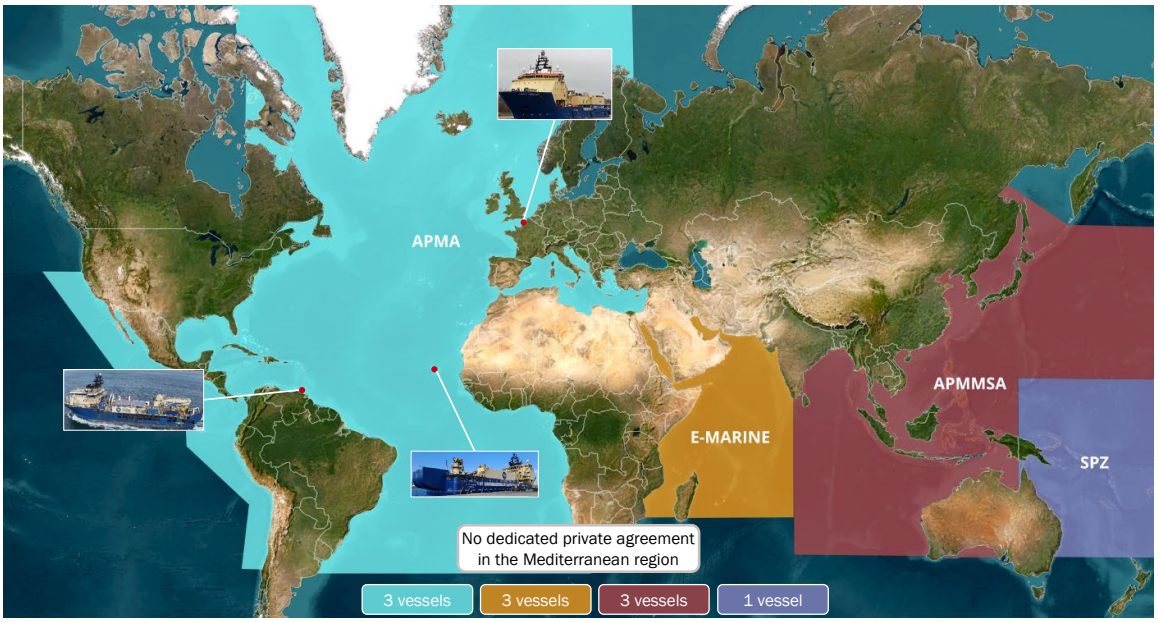
Private maintenance agreements

In this type of agreements, a group of maintenance suppliers offer maintenance services to submarine cable owners on a commercial basis. As opposed to club agreements, costs in private maintenance agreements are **not** transparently shared and the price is commercially negotiated between the cable owner and the maintenance supplier, as well as the SLA.

There are four main private agreements established globally for the maintenance of submarine cable systems, as illustrated in Figure 3.11 below:

- the Atlantic Private Maintenance Agreement (APMA)
- E-Marine
- the Asia Pacific Marine Maintenance Service Agreement (APMMSA), and
- the South Pacific zone.

Figure 3.11: Private maintenance agreements [Source: Analysys Mason, 2025]



Each of these agreements is described in turn below:

- **APMA** – this agreement provides private cable maintenance services in the Atlantic and Mediterranean regions. It relies primarily on three dedicated vessels based in Dunkerque (France), operated by OMS (Singapore), and in Curaçao and Cape Verde, operated by ASN (Europe). APMA is also crucial for the maintenance of European submarine cables.

- **E-Marine** – funded by e& (formerly Etisalat), this private agreement focuses on the Arabian Gulf, the Red Sea and the Indian Ocean. E-marine operates three maintenance vessels based in Hamriya (United Arab Emirates) and Salalah (Oman). Operating in this region represents a challenge as it is heavily monitored by Yemenite Houthis, which were hostile towards Western vessels in 2023 and 2024. ([156])

([156]) Reuters (2024), *Yemen's Houthis say they targeted Western ships*.

- **APMMSA** – this agreement is managed by OMS and ASN, which provide cable maintenance for the Asia–Pacific region. OMS and ASN operate three dedicated vessels based in Jakarta (Indonesia) and Taichung (Taiwan).
- **South Pacific zone** – the South Pacific Marine Maintenance Agreement (SPMMA) covers the southern Pacific up to the Hawaiian Islands. Maintenance is provided by OMS and ASN (acting as partners), which operate a dedicated vessel based in Fiji.

Regional private agreements

As opposed to club and private maintenance agreements, regional private agreements consist of establishing a direct commercial relationship between the cable owner and a maintenance provider. This model is extensively used in the Baltic Sea basin, where a small number of multipurpose companies maintain both power and unrepeated telecoms submarine cables. ([157]) There are three main maintenance providers in the Baltic Sea basin, as listed in Figure 3.7 above.:

- Baltic Offshore (Sweden)
- Lilaco (Finland), and
- Seaworks (Norway).

The unique maintenance arrangement in the Baltic Sea is due to the distinctive characteristics of that basin:

- The vast majority of telecoms submarine cables are relatively short systems, meaning that they are implemented as unrepeated systems. ([158])
- The vessels operate in relatively shallow waters.
- The maintenance providers' vessels and depots are located relatively close to any faults that could occur in the basin, which limits transit time to the fault location.
- No individual permits are required to repair the submarine cables in the Baltic Sea basin, as permits are provided for a term of 1 to 3 years.
- Given the relatively small size of the market, maintenance providers usually use multipurpose vessels for the installation and maintenance of both telecoms and power submarine cables to generate sufficient revenue (the maintenance of telecoms submarine cables would not be sufficient to make these companies economically viable).

In addition to the aforementioned vessels, JD-Contractor A/S (Denmark) has a fleet of four multipurpose vessels which can install and maintain repeated submarine cable systems if required. However, JD-Contractor A/S tends to concentrate on power submarine cables, gas pipeline and windfarm projects.

([157]) The small number of repeated submarine cables in the Baltic Sea basin (for example, C-Lion 1) are repaired under APMA.

([158]) Unrepeated submarine cables do not need any PFE equipment as opposed to repeated systems, which require special skills and a larger vessel to accommodate the potential repair of the PFE.

3.3.4. Main factors influencing installation time

There are several factors that may affect the time required to install a submarine cable, including:

- permits and regulation
- submarine system lead time
- availability of installation vessels
- protection and conflict zones
- weather events.

Each of these are discussed in turn below.

Permits and regulation

As described in Section 3.3.1, operational permits and permits in principle are both required from local authorities to grant access to territorial water and the contiguous zone to lay submarine cables. Permits in principle usually require the provision of the data collected during the seabed survey. In Europe, it typically takes between 10 and 12 months to obtain a permit in principle. However, in the US, it may take as long as 2 to 3 years to secure one of these permits, due to some additional constraints imposed by certain western States.

Therefore, securing a permit in principle often lies on the critical path of a submarine cable installation project, especially for transatlantic cables.

Submarine system lead time

As described in Section 3.3.1, the construction of a submarine cable system involves many components, and timely delivery of the entire system is heavily dependent on the value chain producing each component in time. For example, the fibres need to be first manufactured by one of the three main fibre manufacturers (i.e., Corning, OFS and Sumitomo) before being protected by a water-proof cable (with or without armouring). Depending on the system, the fibre length can span tens of thousands of kilometres, which may result in lead times of several weeks.

Additionally, all active equipment, including the repeaters needed every 80–100 km on a submarine cable system, need to be manufactured. Therefore, for a submarine cable system spanning 10 000 km, more than 100 repeaters will need to be produced. ([159]) As discussed in Section 3.2.3, each repeater needs a laser pump to operate, which is subcontracted to one of two companies in the world (i.e., Lumentum (US) and Coherent Corp (US)). SLTE and transponder equipment also have to be produced for each landing station, although these pieces of equipment are likely to be purchased from a supplier other than the one supplying the wet plant, as explained in Section 3.2.3.

Therefore, scheduling the production of an entire submarine cable system is a complex operation, which requires significant cooperation among different subcontractors, and any delays by one or several subcontractors could potentially be in the critical path of the system being ready for the agreed Ready-for-Service (RFS) date. More generally, the dependence on the supply chain is critical for some components, such as laser pumps and optical fibre, which can only be produced by very few companies.

([159]) Typically produced by the system supplier.

It should be noted that, since a vessel can only install around 5000 km of fibre at a time, the manufacture and assembly of the second vessel load can be done while the vessel is at sea installing the first load.

Availability of installation vessels

Another key factor influencing the installation time of submarine cables is the availability of installation vessels. As explained in Section 3.2.4, less than 25 vessels worldwide can install repeated submarine cables, and vessels have to be reserved a few years in advance. It should be noted that for ultra long-haul submarine cables, several vessels may be required at a time to install the submarine cable system. Finally, it should also be noted that a very large proportion of Subcom's installation fleet is de facto reserved for the installation of Google's submarine cables.

Conflict zones

If a cable needs to be installed in a conflict zone, the installation process can be significantly (or indefinitely) delayed, depending on the conflict duration. For this reason, ongoing conflicts in a region may affect the planned route for laying a submarine cable.

Weather events

The weather is another significant factor affecting the laying of a submarine cable. Cables are preferably laid when adverse weather events are less likely to take place. Bad weather can delay the departure of a laying vessel and can also force the vessel to pause the installation, creating further delays.

3.3.5. Main factors affecting repair time

There are four main factors affecting the repair time of a faulty submarine cable, which include:

- market dynamics and vessel availability
- maintenance contract and maintenance documentation
- spare availability
- permitting and regulation
- weather events.

Each of these factors is examined in the following subsections.

Market dynamics and vessel availability

The global length of submarine cables rose from 0.9 million kilometres in 2010 to 1.8 million kilometres in 2023. Notwithstanding this increase in global cable length, the number of faults remained relatively stable over the same period, at approximately 200 faults per year. ([160]) This means that the average ratio of faults per kilometre of cable laid has consistently decreased. TeleGeography forecasts that the global number of faults will increase to 245 by 2035, and to 285

([160]) International Cable Protection Committee, *Government best practices for protecting and promoting resilience of submarine telecommunications cables*.

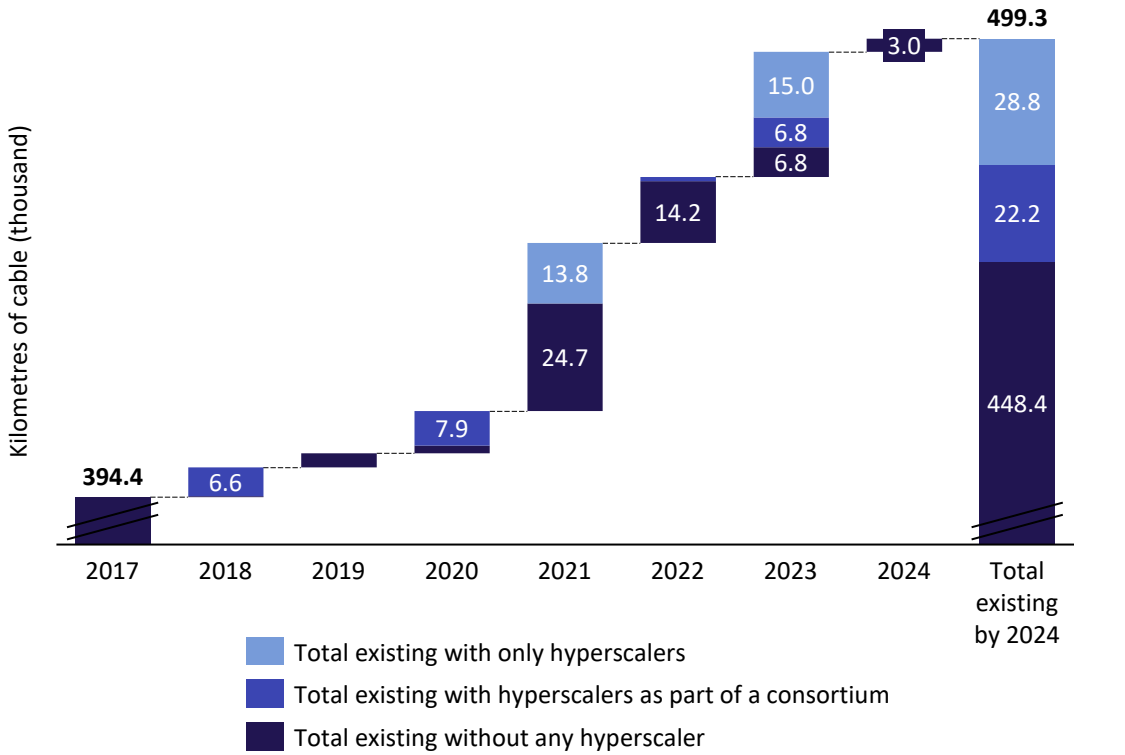
by 2040. ([161]) Importantly, the same report clearly highlights that not all regions in the world will be affected evenly by changes in cable length, nor do faults occur evenly across all regions. For example, the volume of faults in Europe (the East Atlantic Ocean and the Mediterranean Sea) is expected to remain relatively stable (i.e., 48 faults in 2025, rising to 52 in 2035, representing an 8% increase). ([161]) In marked contrast, the number of faults in the Asia–Pacific region (i.e., the Southwest and South Pacific regions) is expected to grow from 90 faults in 2025 to 118 in 2035, representing a 30% increase.

Hyperscaler demand is a major factor influencing submarine cable maintenance, due to:

- the increase in the total submarine cable length to be maintained, driven by the rising demand for submarine cable capacity from hyperscalers as they expand their operations and data needs, especially in the last 5 to 10 years
- maintenance contracts requiring providers to mobilise a significant proportion of their resources
- future maintenance strategy.

As shown in Figure 3.12 below, hyperscalers deployed almost 51 000 km of cable in Europe between 2018 and 2024, representing around 49% of the market in terms of fibre length landing in the EU, and this figure is set to grow in the future. ([162])

Figure 3.12: Submarine cable length deployed between 2017 and 2024 with at least one landing location in the EU [Source: Analysys Mason, 2025]



([161]) TeleGeography (2025), *The Future of Submarine Cable Maintenance Trends, Challenges, and Strategies*.

([162]) Refer to the non-public submarine cable mapping tool developed by Analysys Mason and Axiom.

Hyperscalers' rising demand for submarine cable capacity has also led to Subcom exiting the maintenance market, by converting its last two maintenance vessels into installation laying vessels, following its multi-billion contract with Google. ([163]) Subcom's decision has effectively reduced the global maintenance fleet, but this has had a limited effect on the European market as Subcom was replaced by OMS in the APMA.

The other impact of hyperscalers' growing demand for submarine cable capacity has not yet materialised, but it is a highly likely scenario and could ultimately be the most transformative of all. Hyperscalers may acquire their own maintenance fleet (despite not being their core business) or may secure long-term agreement(s) with cable maintenance supplier(s) on a global scale, which may have an impact on the total number of vessels available for maintaining submarine cables of non-hyperscaler consortia. ([164]) In such long-term agreements, hyperscalers could potentially negotiate lower repair fees by leveraging their scale and accepting slower repairs (i.e., lower-time-to-repair service level agreements) due to the high physical redundancy of their cable routes.

Maintenance contracts and maintenance documentation

It is important to ensure that an appropriate marine maintenance agreement is in place before the RFS date. A marine maintenance agreement provides details of all marine services provided by the vessel operator and stipulates service levels associated with each of these services (including the agreed time to repair the cable in different circumstances). Appropriate service levels are therefore crucial to ensure that the cable will be repaired as quickly as possible to minimise the service outage. In general, there is no real difference in service levels between club agreements and private agreements.

A marine maintenance agreement also defines services associated with the depot and spare equipment. The spares stock should always be maintained in accordance with spares calculations, which define the number of spare parts to be held within the depot based on equipment Mean Time between Failures (MTBF). If a particular component of a submarine cable system fails and no spare is available, it would need to be ordered from the vendor. This process can lead to significant delays in repair and a potentially prolonged service outage. For instance, ordering repeaters from vendors may take up to 12 months, substantially extending the repair time.

One of the key documents in submarine cable maintenance is the Joint System Maintenance Document (JSMD), which provides essential information on the cable systems, fault repair guidelines , and the roles and communication channels among involved parties, among other aspects. If the JSMD is insufficient or unavailable before the RFS date, the likelihood of accidents involving maintenance staff and further delays in cable restoration increases significantly.

Spare availability

Spares stocked in the depots are typically from the submarine cable suppliers. If the required spares are not in the depot, they need to be ordered from the cable supplier, which can take up to 12 months, negatively affecting the time to repair the damaged cable.

Cable designs are proprietary, but all of them are compatible with a technology known as Universal Joint (UJ). As a result, a submarine cable from supplier A can be used to repair a submarine cable

([163]) Subcom (2021), *SubCom announces contract-in-force for Firmina; a new undersea cable system connecting North and South America*.

([164]) Reuters (2023), *Inside the subsea cable firm secretly helping America take on China*.

manufactured by supplier B, provided that the number and type of optical fibre cores inside the cable are compatible.

However, all other main spare parts need to be sourced from the original submarine cable supplier, including:

- **Repeater spares** – repeaters are usually designed specifically for each system, i.e., their optical characteristics (gain, output power and optical filtering) are unique for each submarine cable. A spare repeater from system A cannot be used in system B without a major risk of transmission degradation (even if both systems have been provided by the same supplier).

- **Branching Unit (BU) and Reconfigurable Optical Add-Drop Multiplexer (ROADM) spares** – BU and ROADM spare configurations are commanded by a proprietary protocol and are not compatible across different suppliers. Additionally, there are numerous variations of BU and ROADM, making it unlikely that spares from one system can be used in another, even when supplied by the same vendor (often, systems have more than one spare BU and ROADM to accommodate the use of different configurations throughout the network.

- **PFE spares** – PFE is proprietary and there are no spares per se, only spare cards. Additional spare cards are readily available. The system is sufficiently redundant to run with one PFE down (supported by double- or single-end feeding capabilities). PFE has significant built-in redundancy to ensure operational continuity with a failed card.

These points illustrate that, at present, standardisation of spares is largely limited to the fibre cable itself for jointing purposes, which can pose a barrier in the repair of submarine cables. The standardisation of spare parts could be stocked in the warehouse without having to wait for the submarine cable supplier to provide the proprietary spare parts).

Permitting and regulation

Simplifying the administrative process by local authorities to grant authorisation for site access in territorial waters and the EEZ is a crucial measure to minimise the impact of cable faults.

Streamlining the administrative procedures reduces delays in obtaining the necessary permits and clearances. This ensures that repair teams can access the site promptly, minimising downtime and service disruption.

In general, cable repair times in Asia are significantly longer than in Europe due to the complexities of securing a permit and the requirement in certain Asian countries to use national vessels in territorial waters due to cabotage laws. ([165]) However, this is evolving. For instance, in Malaysia, procedures have been streamlined to allow maintenance companies to repair cables using non-Malaysian vessels. ([166]) Before this change in legislation, maintenance companies were required to justify the use of foreign vessels to repair a cable within territorial waters.

In Europe, the process for obtaining operational permits varies significantly across regions. In the Baltic Sea basin, operational permits are provided for a period of 1 to 3 years, meaning that maintenance providers do not need to request individual permits each time they repair a fault. In marked contrast, the obtention of operational permits in the Atlantic Ocean and the Mediterranean

([165]) ICPC-CIL (2024), *2024 ICPC – CIL Workshop Report: Law of the Sea and Submarine Cables*.

([166]) New Straits Times (2024), *Cabotage policy reinstatement ends years-long debate, boost Malaysia's digital aspirations*.

Sea is often in the critical path to repair faults, ([167]) as operational permits are required for each repair and can take between a few days (for example, in Spain, France, Italy and Greece) and 3 to 4 weeks (for example, in Egypt) for entering territorial waters.

Local authorities can establish clear guidelines and communication channels for cable operators, facilitating faster coordination during fault incidents. Additionally, dedicated points of contact within the local government can further accelerate the authorisation process.

Weather events

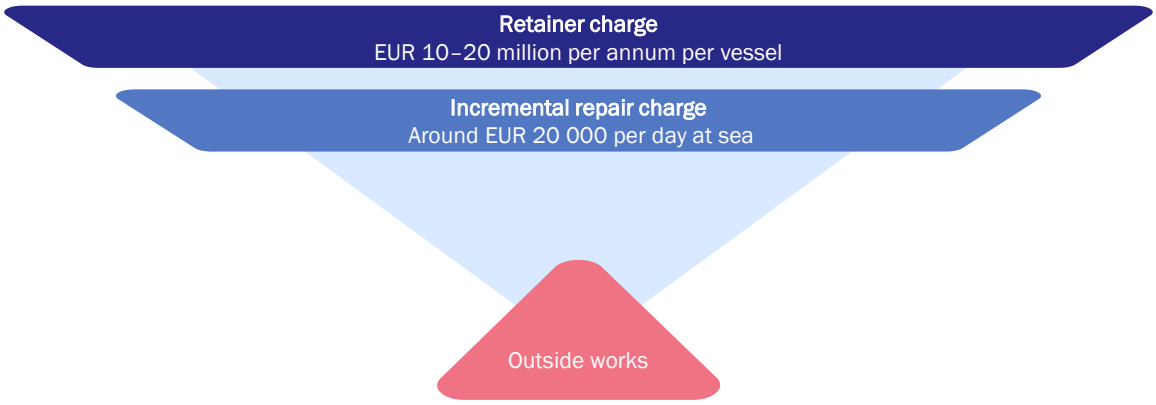
Weather conditions can significantly affect the time it takes to repair a cable, including:

- delaying the vessel transit to the repair site
- damaging the vessel
- delaying the repair operations while on site.

3.3.6. Maintenance and installation revenue models

The typical revenue model for maintenance vessel owners under a club maintenance agreement consists of an annual retainer charge supplemented by an incremental variable charge for the actual services. In addition, when allowed by the maintenance contract, maintenance vessel owners complement their revenue by undertaking smaller activities (laying of small submarine cables), which is generally referred to as 'outside works'. This model is illustrated in Figure 3.13, below.

Figure 3.13: Typical revenue model for vessel owners under a club maintenance agreement [Source: Analysys Mason, 2025]



Retainer charge

The retainer charge covers the fixed costs associated with the vessels (including maintenance costs, assurance costs and rental costs for the depot, among other elements), as well as the retainer for the crew to ensure that the necessary personnel are readily available to perform maintenance activities. The retainer charge typically ranges from EUR 10 million to EUR 20 million. ([168])

([167]) Based on data provided by maintenance providers which is deemed commercially sensitive and could not be explicitly included in this report.

([168]) Source: Axiom.

For club maintenance agreements, the retainer cost is transparently shared between consortium members based on the relative length of their cables. This means that owners with longer cable lengths will pay a higher retainer charge than those with shorter cable lengths.

For private maintenance agreements, vessel owners directly charge customers based on the length of their cable and depending on the number of customers sharing the same maintenance vessel within the same geographical area. As opposed to club maintenance agreements, the charge is not transparent in private maintenance agreements.

If no maintenance or repair work is needed throughout an entire year, cable owners would only have to pay the retainer charge.

Incremental repair charge

Each time a vessel is sent to perform a repair on a submarine cable, an incremental repair fee is requested from the owner of the faulty cable. This incremental fee is usually around EUR 20 000 per day at sea. This fee excludes any expenses such as fuel costs, which need to be paid on top of the repair charge by the owner of the faulty cable. The fee also excludes any equipment and spares needed to repair a fault.

Once the maintenance vessel is out at sea, there are usually no provisions for delays in the repair process. That is, the owner of the faulty cable needs to pay a daily charge for each day the vessel is at sea, even in the event of a storm or other unforeseen event which may cause a delay in the repair work.

Under the club and private maintenance agreement models, the total repair cost for a single fault is typically between EUR 0.5 million and EUR 1 million, ([168]) depending on how far the vessel has to travel and the complexity of the fault.

Outside works

To complement their revenue during periods of low activity, maintenance vessels may conduct other works that fall outside the scope of their maintenance agreements (outside works). Outside works are also of interest for club maintenance agreement members, as any incremental revenue generated from these activities is often shared among the members (for example, a reduction in the retainer charge). However:

- not all maintenance agreements allow outside works to be performed
- some maintenance agreements only permit outside works for a specific period of time (for example, up to 3 months per year).

3.4. Analysis of the submarine cable vessel fleet

Vessels used to install and maintain submarine cables are divided into three main categories based on their intended function:

- telecoms submarine cable vessels (telecoms vessels)
- power submarine cable vessels (power vessels)
- hybrid multipurpose submarine cable vessels, used for the installation of both power cables and telecoms submarine cables (hybrid vessels).

Each of these vessel types is discussed in turn below, particularly focusing on telecoms vessels, which are of particular interest for this report.

3.4.1. Telecoms vessels

Telecoms vessels can be divided in two main categories: cable installation vessels and cable maintenance vessels, with a global fleet comprising 53 vessels, capable of maintaining and/or installing **repeated submarine cable systems**. ([169]) Cable installation and cable maintenance vessels are designed to serve a specific function, making them distinctly different.

Cable installation vessels

Cable installation vessels, also known as cable laying vessels, are equipped with tanks to store the fibre submarine cable to be deployed, which can be up to 5000 km long at a time. ([170]) Cable installation vessels usually have plough burial capabilities to bury the cable in shallow water to mitigate against adverse human actions (for example, fishnets snagging the cable, dredging, etc.). Some installation vessels have a burial capability of up to 3 metres deep, which means that cable installation vessels are more energy demanding than maintenance vessels.

As of 2024, the global fleet included 24 installation vessels from 11 different providers, capable of installing repeated submarine cable systems (see Appendix B). The top-two providers (Subcom and ASN) collectively own a total of 12 vessels, representing 50% of the global cable laying fleet. Subcom owns eight cable laying vessels, which represents more than one third of the global fleet. Subcom recently repurposed its last two maintenance vessels to installation vessels to meet Google's growing demand for submarine cable deployments, as Subcom is Google's preferred partner for cable supply and installation. ([171]) This means that Subcom has effectively exited the maintenance market.

ASN is the second-largest cable laying vessel owner, with four vessels, representing 17% of all cable laying vessels worldwide (see Appendix B).

It should be noted that all installation vessels could perform maintenance activities; however, they are significantly less efficient due to their higher running costs compared to those of maintenance vessels.

The global installation fleet has an average age of 24 years, with 87% of the vessels being older than 20 years, as illustrated in Figure 3.14. Both Subcom and ASN installation vessels were all constructed before 2004, ([172])([173]) which means they will reach end-of-life by 2040 (see Appendix B). Based on Figure 3.14, globally, 9 installation vessels will need to be replaced in the next 10 to 15 years.

([169]) There are other smaller hybrid vessels capable of installing and maintaining small unrepeated submarine cable systems; these are covered in Section 3.5.3.

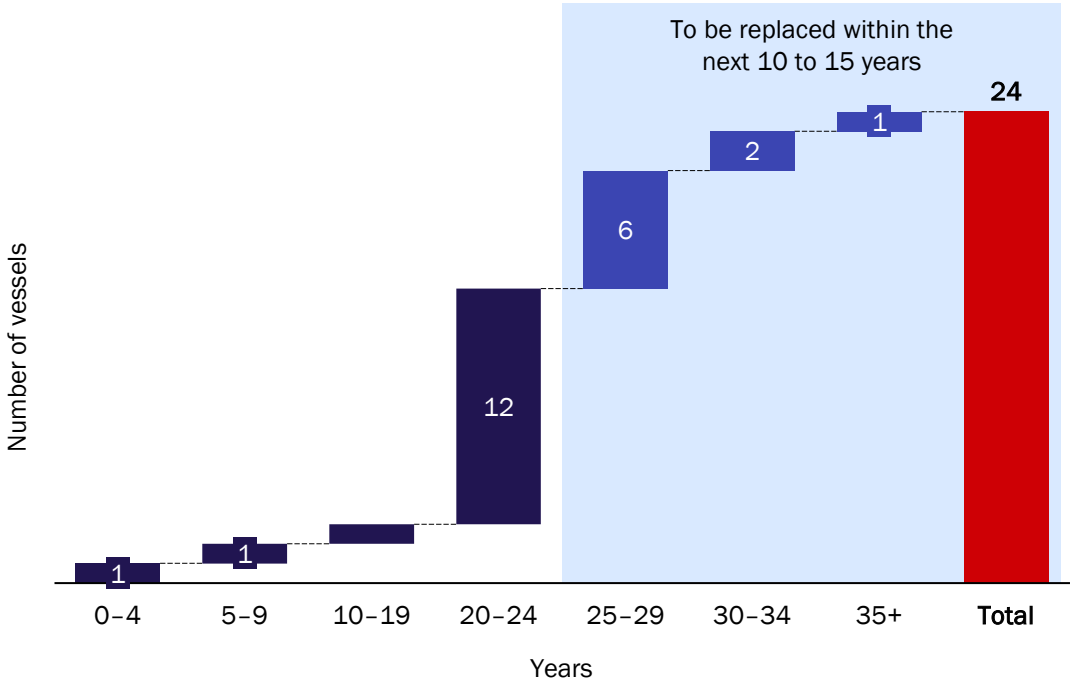
([170]) The total length of telecoms submarine cables can exceed 20 000 km (for example, 2Africa and SEA-ME-WE 3/5/6), but vessel tanks only have the capacity to deploy 5000 km at a time.

([171]) The Verge (2024), *The cloud under the sea*.

([172]) Except for Global Sentinel, which was built in 1991 and will reach end-of-life 10 years before the rest of the Subcom fleet (i.e., by 2031).

([173]) Ile d'Yeu was retrofitted from a maintenance to a cable laying vessel.

Figure 3.14: Age distribution of the global cable installation fleet [Source: Analysys Mason, 2025]



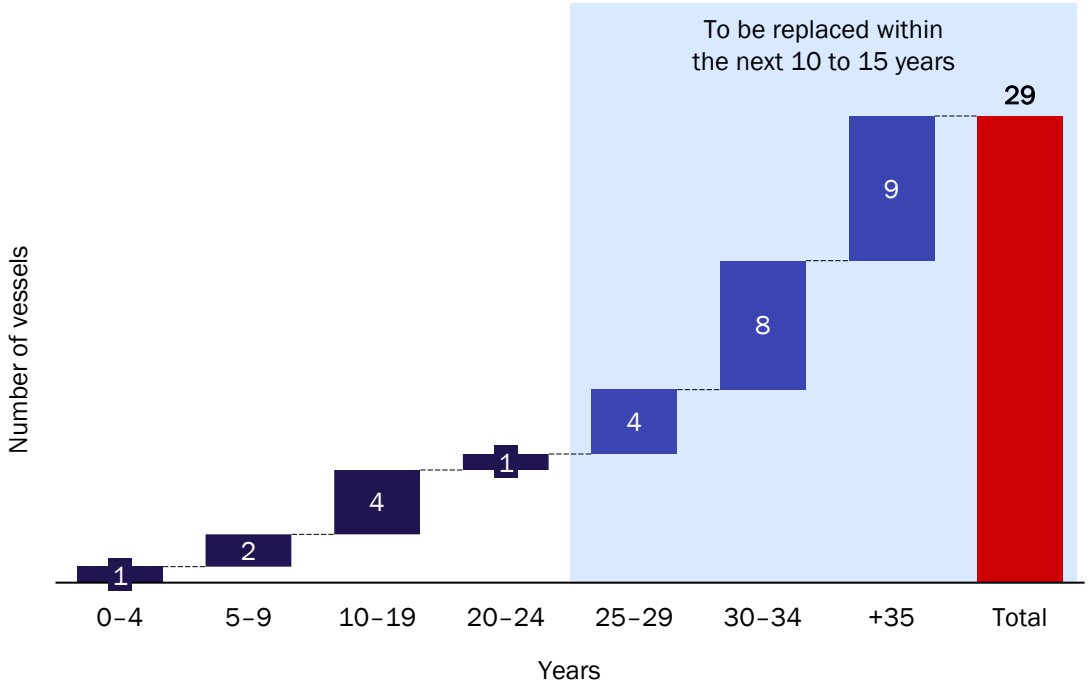
Cable maintenance vessels

Cable maintenance vessels are designed to be flexible and have a relatively lower fuel consumption than cable installation vessels, which helps to reduce running costs. This efficiency is achieved because maintenance vessels do not need to transport a high load and do not have the power to perform plough burial activities, which require significant energy.

As of 2024, the global fleet of maintenance vessels included 29 vessels from 14 different providers (see Appendix C). The top-five maintenance suppliers (ASN, Orange Marine, OMS, Global Marine and E-Marine) collectively own 17 vessels, representing 59% of the global maintenance fleet.

The global fleet of maintenance vessels has an average age of 29 years. Appendix C shows that nearly 60% of the maintenance fleet is 30 years or older, and only seven vessels are less than 20 years old. It should be noted that Orange Marine owns some of the most recent vessels, including Sophie Germain and Pierre de Fermat, built in 2023 and 2014, respectively.

Figure 3.15: Age distribution of the global cable maintenance fleet [Source: Analysys Mason, 2025]



The initial observation is that the global maintenance fleet is significantly older than the global installation fleet, which is partly attributable to installation vessels being repurposed as maintenance vessels when they reach a certain age.

Based on the above analysis, globally, **21 maintenance vessels** will need to be replaced in the next 10 to 15 years (at least to maintain current capacity). The options and associated costs of replacing end-of-life vessels are analysed below.

3.4.2. Power vessels

This report primarily focuses on telecoms submarine cables and their associated vessels. However, to enable comparison with the power submarine cable industry and explore potential synergies, this section examines power submarine cable systems, power vessels and the associated ecosystem.

Power vessels are fundamentally different from telecoms vessels, as illustrated in Figure 3.16.

Figure 3.16: Comparison between power and telecoms submarine cables and associated vessels [Source: Analysys Mason, 2025]

Category	Telecoms cable project	Power cable project	Comments
Project characteristics			
Total cost of project (EUR)	50 million to lay a telecoms cable between Ireland and France	1600 million to lay a power cable between Ireland and France	The budget for power cable projects is approximately one order of magnitude greater than for telecoms cable projects
Project timeframe	Typically 2–3 years	Typically 5–6 years	
Cable characteristics			
Cable length	Up to 10 000 km	Up to 1000 km	
Cable diameter	2–5 cm	20–40 cm	
Joints	1 m long	10 m long	Telecoms benefits from Universal Joint Consortium
Ship characteristics			
Cable tank design	Fixed cable tank	Rotating cable tank	Rotating tanks are needed for very rigid power cable
Cable tank capacity	5000 km	100 km	
Running costs	Designed to be efficient	Significantly higher running costs	Power cable laying vessels consume more fuel than those used for laying telecoms cables
Cost			
Cost per day (cable laying, EUR)	150 000	300 000	Using a power cable laying vessel costs twice as much as a telecoms vessel
Maintenance model			
Maintenance	Either club or private	Maintenance with cable supplier	
Key suppliers	ASN, Orange Marine, Global Marine, OMS, etc	Nexans, Prysmian, Jan de Nul	
Repair time (on site)	24 hours	1 week	Telecom joints are 1 m long, compared to 10 m long for power joints

Characteristics of power vessels compared to telecoms vessels

Power vessels are significantly larger than telecoms vessels because power cables are much heavier on a per-metre basis than telecoms submarine cables due to their larger diameter, and because the cable is made of heavy metal conductor and not glass fibre. The other main difference is that vessels used to install submarine power cables need to be fitted with a rotating cable tank to minimise the torque generated during installation on the rigid power cable. Telecoms vessels, on the other hand, install telecoms submarine cables using fixed tanks.

Power vessels are significantly more costly to build than telecoms vessels due to their considerably larger dimensions and greater complexity. In addition, larger vessels also entail higher operational costs, partly because they consume more fuel and require a larger crew.

Consequently, the average cost to hire a power vessel for the installation of a power submarine cable is typically twice as high as the cost of hiring a telecoms vessel (i.e., EUR 300 000 per day for a power vessel versus EUR 150 000 per day for a telecoms vessel). ([174]) Therefore, it would not be economically viable to use power vessels to install (or repair) telecoms submarine cables.

Furthermore, it should be noted that it is challenging to equip a telecoms vessel with power cable repair capabilities, as the vessel would need to support higher load and be fitted with a rotating tank, which may take up to 2 months to install on an existing vessel ([175]) (provided it is available in the first place).

Most importantly, the repair process of telecoms submarine cables is highly dependent on getting access to the submarine cable spares at the depots and the specialised crew. These challenges typically constitute the highest barriers to using power vessels for the installation and repair of telecoms submarine repeated cables.

However, it should be noted that, in small basins, multipurpose vessels do exist, but their use is typically limited to the deployment and maintenance of small unrepeated cables in shallow water, as explained in Section 3.4.3.

The power submarine cable market and operations

The power submarine cable market has historically been dominated by four Tier 1 suppliers ([176]) (Prysmian, NKT, Nexans and Sumitomo Electric). However, some Tier 2 suppliers are starting to play a more prominent role in the market, as shown in Figure 3.17.

([174]) This does not include fuel costs, which are charged separately and are expected to be significantly higher for a power vessel than for a telecoms vessel, due to greater fuel consumption.

([175]) Source: Axiom.

([176]) Tier 1 suppliers are the larger suppliers in the market. Tier 2 suppliers tend to address niche requirements in the markets and are smaller than Tier 1 suppliers.

Figure 3.17: Submarine power cable suppliers [Source: Analysys Mason, 2025]

prysmian

- **Ownership and funding:**
  - public company listed on the Milan Stock Exchange, with over 81% share owned by institutional investors
- **Submarine system capability:**
  - power generation, transmission and distribution, and telecoms systems

NKT

- **Ownership and funding:**
  - the NKT A/S share is 100% free float, with 53% of the share capital registered by Danish shareholders
- **Submarine system capability:**
  - high, medium and low-voltage cable solutions

Nexans

- **Ownership and funding:**
  - public company listed on the Paris Stock Exchange, with major shareholders from Chile, France and the UK
- **Submarine systems capability:**
  - power generation, transmission and distribution

SUMITOMO ELECTRIC

- **Ownership and funding:**
  - major shareholders include other companies within the Sumitomo Group, as well as domestic and international institutional investors
- **Submarine systems capability:**
  - power generation, transmission and distribution, and telecoms systems

HENGTONG

- **Ownership and funding:**
  - publicly traded company, with Hengtong Group being its largest shareholder (24%)
- **Submarine system capability:**
  - power and telecoms cables and systems

ZTT

- **Ownership and funding:**
  - the ownership structure includes a mix of institutional investors and the founding family
- **Submarine system capability:**
  - power (high-voltage and medium-voltage) cable solutions, and telecoms cables and systems

LS Cable & System

- **Ownership and funding:**
  - the company is privately held and controlled by the Koo family, who are the founding family of the LG Group
- **Submarine systems capability:**
  - power and telecoms cables and systems

ABB

- **Ownership and funding:**
  - publicly traded company with Investor AB from Sweden as major shareholder, holding about 14% share
- **Submarine systems capability:**
  - power cable systems and accessories

It is important to highlight that Europe holds a leading position in the submarine power cable industry, as three of the four main Tier 1 suppliers are European companies.

The maintenance market for submarine power cables is not as mature as the submarine telecoms cable maintenance industry, for several reasons:

- the repairs are specific to the cable supplier, hence only the cable supplier can repair its own cable
- the volume of submarine power cables is significantly lower than that of telecoms cables, meaning that the installation and maintenance fleet is much smaller
- the availability of spare parts (such as spare cable) in depots is very limited and each cable repair is customised (not industrialised).

Nexans and Prysmian both have modern power cable laying vessels, ([177])([178]) however, most submarine power cable system suppliers do not own any installation or maintenance vessels. Instead, power submarine cable suppliers tend to subcontract large vessel provider companies such as Jan de Nul ([179]) to maintain and/or deploy power submarine cables.

3.4.3. Hybrid vessels

As discussed in Section 3.3.3, vessel owners tend to use hybrid vessels which can install and/or maintain both power and telecoms submarine cables in small sea basins (for example, the Baltic Sea), due to the relatively small size of the installation and repair market in these areas. This is because vessel providers have to offer services to both power and telecoms submarine cable owners to generate sufficient revenue and be economically sustainable.

It should be noted that, in smaller basins, the short distances to travel to the repair site, coupled with the shallow depth of water and the simpler nature of the submarine cable systems to be repaired (i.e., unrepeated systems), mean that hybrid vessels are significantly smaller than those used in larger and deeper basins (for example, the Atlantic Ocean) and are unsuitable for use in larger basins. These vessels are also sometimes used to support the installation or maintenance of offshore wind farms.

3.4.4. Maintenance fleet by European region

As outlined in Section 3.1, Member States are connected together through a number of submarine cable routes, which can be categorised into four different geographical regions. These regions are served by the following vessels:

- three ACMA vessels (two operated by Global Marine ([180]) and one operated by Orange Marine) ([181])
- two MECMA vessels (one operated by Elettra and one by Orange Marine)

([177]) Nexans, *Cable laying vessel Nexans Aurora*.

([178]) Prysmian, *Prysmian Group presents the most advanced cable laying vessel "Leonardo da Vinci*".

([179]) Jan de Nul, *Fleet*.

([180]) Due to the recent acquisition of Global Marine by Keppel Fund (Singapore), there is a risk that the vessel based in Portland (UK) (serving ACMA) could be relocated to Asia.

([181]) It should be noted that vessels that are part of APMA and ACMA that are based in Curaçao mainly serve the West Atlantic coast, and tend to serve the European Atlantic region when vessels which are based in European locations are already in use.

- three APMA vessels (two operated by ASN and one operated by OMS)[181]
- four hybrid vessels in the Baltic Sea ([182]) operated by Baltic Offshore (two vessels), Lilaco (one vessel, Finland) and Seaworks Norway (one vessel).

Therefore, eight maintenance vessels serve the large basins (i.e., the Atlantic Ocean, including the North Sea/Channel and the Mediterranean Sea), and over four smaller hybrid vessels serve the Baltic Sea.

The average age of the eight maintenance vessels serving repeated submarine cables in large basins across transatlantic and European waters is 20 years, which is 9 years below the average age of the global fleet (see Figure 3.18). Three of these vessels will need to be replaced in the next 10 to 15 years.

Figure 3.18: Age distribution of European maintenance vessels used in large basins [Source: Analysys Mason, 2025]

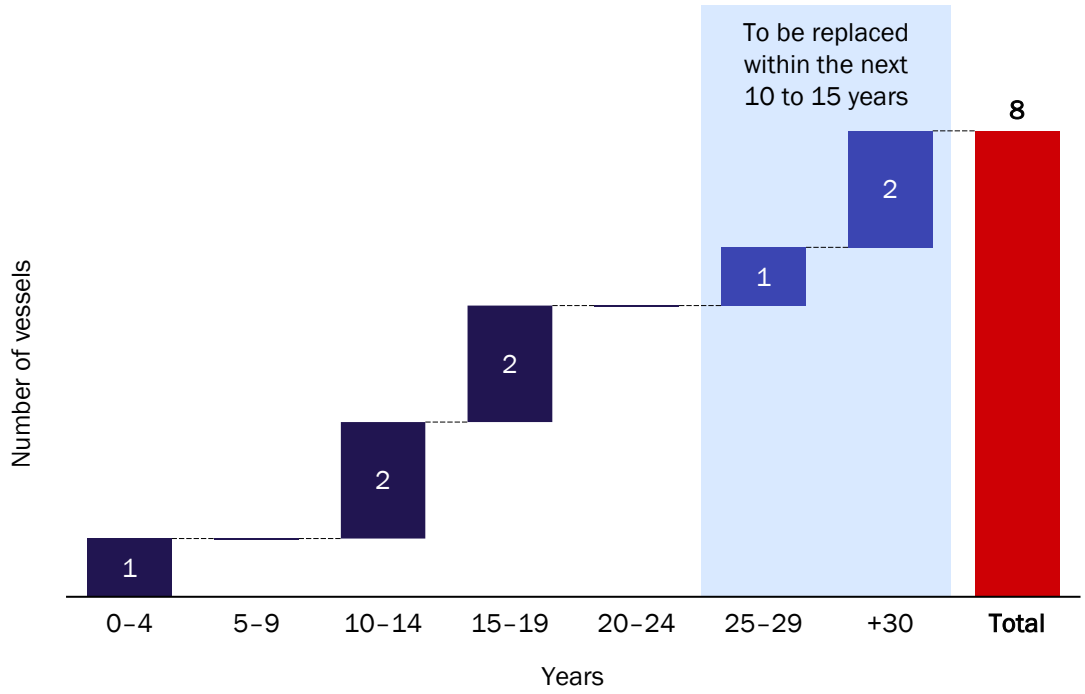
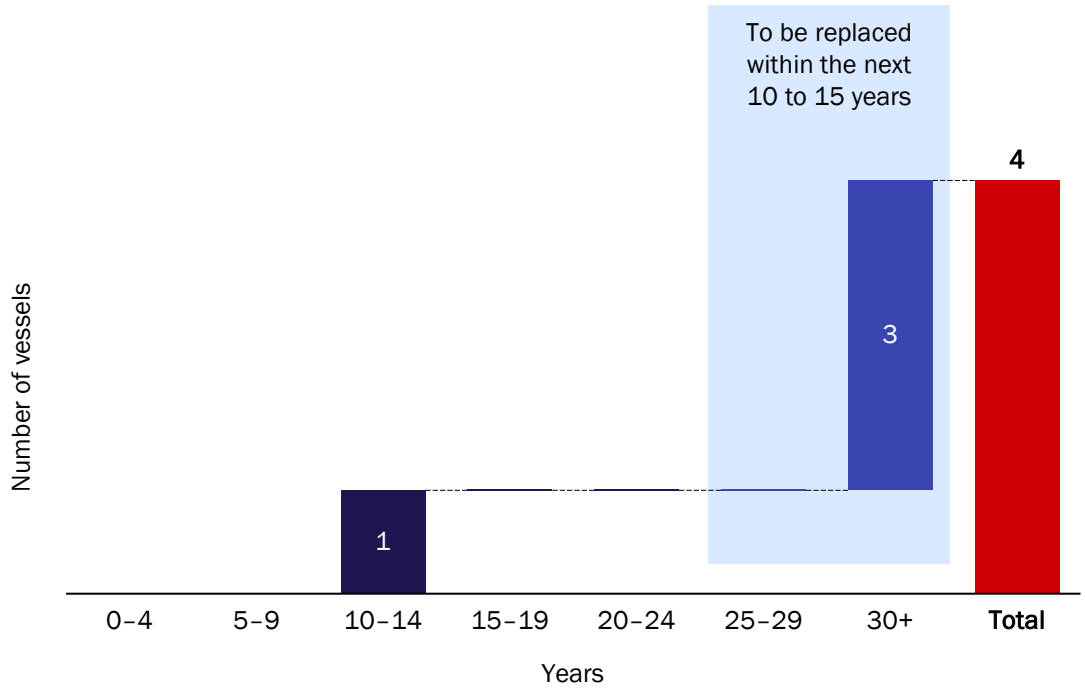


Figure 3.19 provides the age distribution of hybrid vessels serving the Baltic Sea basin. The average age of the four hybrid vessels serving unrepeated cables in the Baltic Sea is 38 years, which is significantly above the average age of European maintenance vessels. As shown in Figure 3.19 below, the majority of these vessels (three out of four) will require replacement in the next 10 to 15 years.

([182]) This is not an exhaustive list of vessels but provides examples of maintenance providers in the Baltic Sea basin.

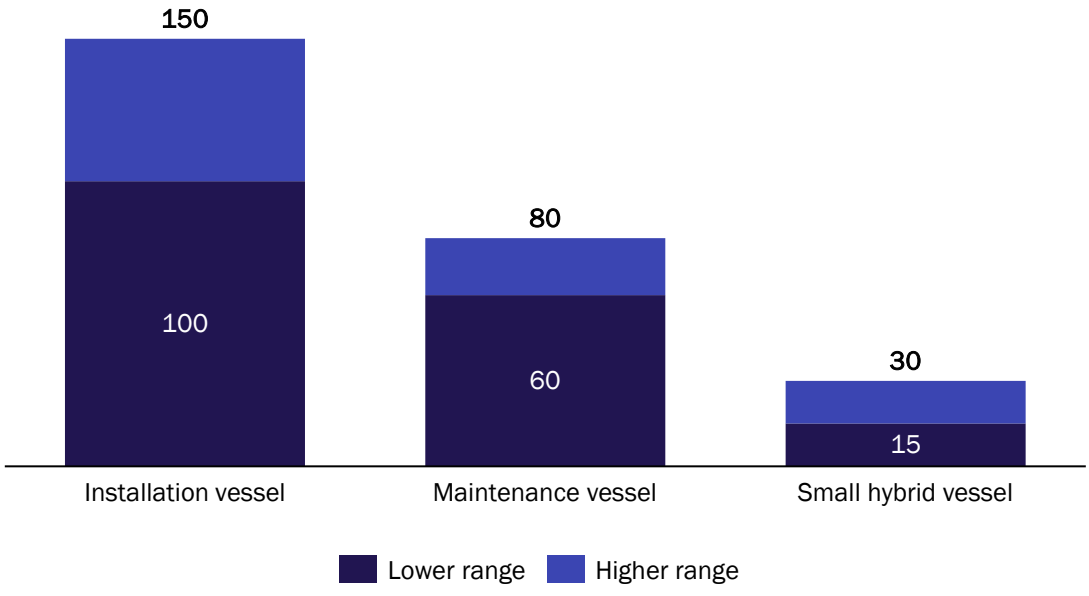
Figure 3.19: Age distribution of hybrid vessels serving the Baltic Sea [Source: Analysys Mason, 2025]



Vessel replacement costs

The lifetime of a vessel is estimated to be between 35 and 45 years if it is regularly maintained. Therefore, in the rest of this report, we will assume that when a vessel reaches this timeframe, it needs to be replaced. Figure 3.20 shows the cost of replacing maintenance and installation vessels.

Figure 3.20: Cost ranges for replacement of installation and maintenance telecoms vessels used in large basins [Source: Analysys Mason, Axiom, 2025]



As shown in Figure 3.20, as of 2025, a cable installation vessel costs nearly twice as much as a maintenance vessel.

Based on the age analysis of the installation and maintenance fleet conducted above, it is evident that significant investment will be required in the next 10 to 15 years, and planning for these capital expenses will be essential to maintaining an effective installation and maintenance capability for submarine cables.

Considering the global maintenance fleet, 21 vessels will need to be replaced in the next 10 to 15 years, at a unit cost of between EUR 60 million and EUR 80 million. This represents a capital cost between EUR 1.3 billion and EUR 1.7 billion (nominal value).

With regard to the maintenance fleet serving Europe, three maintenance vessels serving large basins will need to be replaced in the next 10 to 15 years, requiring between EUR 180 million and EUR 240 million (nominal value) of investment by maintenance suppliers to sustain the current size of the fleet in ACMA, APMA and MECMA.

Regarding hybrid vessels serving the Baltic Sea, the unit cost of replacing these vessels is estimated to range between EUR 15 million and EUR 30 million, as they are significantly smaller than the vessels serving larger basins. As a result, the majority (three) of hybrid vessels that have been identified in this report will need to be replaced in the next 10 to 15 years, requiring capital expenditure (capex) in the range of EUR 45 million to EUR 90 million (nominal value).

Therefore, accounting for maintenance vessels in large basins and for hybrid vessels in the Baltic Sea, a total capex of between **EUR 225 million and EUR 330 million** would be needed in the next 10 to 15 years to sustain the current size of the European fleet .

Given the relatively small margins generated by the submarine cable maintenance industry, ([183]) the business case for investing in new vessels is challenging for maintenance providers. As a result, new governance models are emerging to fund the replacement capex. For example, global investment firm KKR acquired some equity in OMS in October 2024, in exchange for a USD 400 million (approximately EUR 380 million) commitment to fund the next generation of vessels for OMS. ([184]) New funding models will also be required for other maintenance providers to purchase replacement vessels, to continue supporting European maintenance agreements with the same fleet volumes, while alternative sources of funding may also be required to sustain the maintenance industry.

Finally, the relatively short-term duration of maintenance contracts (i.e., typically spanning 3 to 5 years, with a 6-month notice period) does not incentivise maintenance suppliers to invest, and longer-term contracts may be required to support the purchase of new vessels.

([183]) Besch, S. and Brown, E. (2024), *Securing Europe's Subsea Data Cable*.

([184]) Reuters (2024), *KKR-backed Malaysian group OMS signs contract for cable-laying vessels with Dutch firm*.

3.5. Submarine cable funding models

Submarine cable systems, like other large infrastructure projects, involve significant upfront costs which are recovered over the design life of the project (25 years). Regardless of the composition of the project, over 55–60% of all costs (i.e., capex and opex) are incurred before the cable is RFS. ([185])

Sufficient funding is required at the beginning of the project to cover the cost of building the submarine cable and to manage the cashflow during the initial years. Before the submarine cable is RFS, the special purpose vehicle (SPV) created specifically to finance, build, own and/or operate the submarine cable will need to finance the deployment capex, as well as the costs associated with fronthaul and backhaul infrastructure, and staffing. Once the submarine cable is RFS, the SPV will need sufficient funding to cover operation and maintenance costs, which will eventually be covered by revenue once capacity sales exceed running costs.

All stakeholders aim to minimise upfront funding requirements, often mitigating risk by securing pre-commitments from anchor tenants (early customers) in the form of indefeasible rights of use (IRUs) leasing capacity for 10, 15 or 20 years, in exchange for significant price discounts on the price paid by customers who purchase capacity post-construction.

Lease costs for the entire duration of the IRU (10, 15 or 20 years) are paid to the cable owner upfront, with only maintenance and operating costs paid annually by the customers. Securing a significant number of IRUs minimises the market risk and is a key requirement to unlock investment from private financiers.

3.5.1. Project partners and project structure

Project partners can include telecoms companies, hyperscalers, governments (directly or indirectly through government companies and foundations), investors and development banks.

These various stakeholders come together to organise and deploy a submarine cable project using different approaches, depending on factors like the funding model, ownership structure and operational responsibilities. Some of the most common approaches are listed below:

- **Consortium (also known as a 'joint build partnership')** – a consortium involves multiple companies coming together to deploy a submarine cable, and each member of the consortium owns a portion of the cable system. The consortium members earn their financial return by exploiting their portion of the submarine cable within their broader telecoms operations.
- **Private ownership –** a private company funds and owns the submarine cable. This may include investors that have identified an opportunity in the market and deploy a cable for profit. It may also include an hyperscaler which needs to deploy a submarine cable for their own connectivity requirements to efficiently move vast amounts of data around the globe (for example, to connect different cloud regions).
- **Public–private partnership (PPP)** – this is a long-term agreement where a government entity works together with private companies to build and manage submarine cable systems for strategic reasons.

Each of these approaches is discussed in turn below.

([185]) Source: Analysys Mason, Axiom.

Consortium

Historically, the vast majority of submarine cable systems were deployed and operated under a consortium model where the risks and costs were shared by each member of the consortium. Consortium members were typically telecoms operators. Although the model is still used (for example, IEX, 2Africa, Africa1 and SMW6), many new submarine cable systems have taken other approaches.

Each consortium member invests in the project as a co-owner and receives a share of capacity on the system that is proportional to its equity investment. In return, each consortium member commits to covering a corresponding portion of the upfront capital costs, as well as the operation and maintenance expenses over the system's lifetime. Each consortium member develops its own business plan to support its decision to invest in the cable system:

- There is no single business model for the overall submarine cable system. Each carrier has its own business plan for its allocation of capacity, which is part of their carrier core business plan.
- The consortium members sign a Memorandum of Understanding (MoU) to develop the configuration of the cable system, investment and ownership rules, capacity allocation principles, and operation and maintenance cost sharing. These rules and principles are then transcribed in the co-ownership agreement, usually referred to as the construction & maintenance agreement (C&MA) or joint build agreement (JBA).
- The consortium membership list is closed as soon agreements are reached on cable system configuration, on sharing ownership principles and on funding. As a consequence, the investment shares committed by all consortium members must total 100% of the system capital cost.

Private cables

In the past, private cables were wholly owned through SPVs. These were commercial structures used as investment vehicles responsible for building, owning, operating, maintaining and selling (or leasing) the infrastructure. Today, most private cables are supported by a mix of funding sources, including sovereign wealth funds and hyperscalers, with SPVs still commonly used as intermediaries for managing the investment.

Private cables are often set up to profit on the commercial opportunity created by underserved growing demand in specific regions or countries. The revenue secured by the SPV forms the basis of the return for investors.

Hyperscalers are key players in the private cable industry, moving from being an anchor tenant to becoming cable owners in less than a decade. Their core business involves moving large volumes of data globally between their data centres via submarine cables. This in turn means that they invest in and frequently build cables themselves as part of their core business. The core business requirement dictates the route of the submarine cable and the location of landing stations, and is directly linked to hyperscalers' revenue source.

Public–private partnership

In the submarine cable industry, a public–private partnership (PPP) typically refers to cables which are fully (or partly) funded using strategic public funding. In addition, a PPP may include non-financial support, such as the provision of land rights and favourable regulation.

In some cases, where submarine cables are not commercially viable, governments and other public entities may invest in and/or grant aid to a project. In these cases, public bodies often take a more strategic view of connectivity considering the wider economic development of other industries that depend on the availability of reliable, resilient and fair-priced international connectivity.

The involvement of public entities in private projects, in particular complex international telecoms projects, generates benefits across the whole value chain. In this regard, infrastructure providers can benefit from access to public funding and land rights; network operators and Internet Service Providers (ISPs) benefit from access to shared infrastructure at lower costs with reduced risk; consumers and end users benefit through more resilient internet access, lower latency and increased competition; while governments and regulators advance key policy goals such as digital sovereignty and economic development. Considering that government's incentives relate to public welfare rather than personal profit, PPPs tend to enhance the feasibility of higher-risk projects with lower return expectations.

The involvement of private players also reduces the project risk for the public sector, as it ensures a higher quality of service and some anchor customers. By combining public financing and regulatory support with private-sector innovation, operational expertise and investment discipline, PPPs can reduce the overall lifecycle costs (total cost of ownership) of submarine cable projects. They can increase the financial viability of these projects and deliver more affordable international connectivity, particularly for underserved regions.

Examples of public funding in Europe include the use of the CEF programme, which can fund up to 30% of the capital costs of European cables. All CEF funding is grant funding and, although its drawdown is subject to programme conditions, the EU is different to other co-investors as they do not expect a financial return on their investment. CEF funding can be increased to up to 50% for cross-border projects (or up to 70% for the Outermost Regions (ORs) and Overseas Countries and Territories (OCTs) of the EU). Projects that have received CEF funding include the SwePol Link submarine cable connecting Sweden to Poland, the Far North Fiber cable linking Europe and Asia through the Arctic region, and the PISCES cable connecting Ireland, France, Portugal and Spain, among other projects.

3.5.2. Financing of projects

The funding of submarine cable projects depends on the partners involved and their motivation. Similar to most infrastructure projects, options include direct funding through shareholder equity and self-finance, pre-RFS sales, as well as debt.

Debt financing can be an important part of the mix, enabling partners to enjoy a higher return on investment (RoI), and it can also contribute to tax minimisation. However, senior debt is usually conditional on significant pre-sales (typically a minimum of 50% of the debt).

Hyperscalers have become direct investors in new submarine cable systems, either through a consortium approach or, increasingly, through single or limited multi-party ownership.

Multilateral institutions (such as the World Bank and its affiliates, the Asia Development Bank and the EIB) also play a role in financing new projects, particularly in situations where the business case for a new system that will provide connectivity to remote and not densely populated regions may be challenging (for example, various projects connecting island territories in the Pacific). ([186])

Government institutions may sometimes be involved in national or regional systems by providing subsidies, grants and promotional loans.

([186]) Center for Indo-Pacific Affairs (2024), *Improving Public-Private Partnerships on Undersea Cables: Lessons from Australia and Its Partners in the Indo-Pacific.*

3.5.3. Publicly funded repair and maintenance of submarine cables

Beyond the allocation of publicly funded support for the submarine cables themselves, it may be possible to publicly fund their repair and maintenance. Options include funding the replacement of ageing vessels or co-financing maintenance agreements. Given the strategic nature of such investments, State aid may be an option in the same way that CEF funding is available to financially support CPEIs. The combination of the two was already highlighted in Recommendation (EU) 2024/779.

As outlined above, the entire maintenance fleet in the seas and oceans of interest is privately owned. It is estimated that between EUR 225 million and EUR 330 million of replacement capex will be required in the next 10 to 15 years to ensure the current size of the maintenance fleet in Europe. There are also challenges associated with covering the costs of operating the maintenance fleet.

The implications of public investment for replacing the ageing fleet of maintenance vessels or purchasing new vessels will need careful consideration in terms of the impact that this may have on the market. A key challenge in allocating publicly funded support for the repair and maintenance of submarine cables is ensuring that such investment does not distort the market and undermine its long-term viability. For example, publicly funded vessels could displace some of the privately funded existing vessels, merely replacing the funding source while maintaining the current level of coverage (or potentially even reducing it further).

The current structure of the submarine cable market, which features different maintenance agreements and private agreements, means that any investment scheme needs to be carefully examined through consultation with key stakeholders, but it should be possible to partly fund aging vessels.

4. MAPPING OF CABLE INFRASTRUCTURE IN THE EU

Recommendation (EU) 2024/779 requires the Expert Group to map the existing and planned submarine cable infrastructures at EU level. This section outlines the implementation of this mapping exercise and analyses the existing and planned infrastructure to identify potential gaps. It starts by describing the methodology used to map existing and planned cables, followed by an overview of Europe's cable infrastructure. A fault analysis is then conducted across each European region. Subsequently, all key landing stations are listed and all main cloud regions in Europe highlighted, where hyperscaler data centres are located and require connectivity. To conclude, potential gaps are identified.

4.1. Methodology to map submarine data cable infrastructures

The Contractor (Analysys Mason and Axiom) was commissioned by the Expert Group to create a map of the existing and planned submarine cables with at least one landing station at EU level (non-public). To achieve this objective, several sources of information have been consulted by the Contractor, including Analysys Mason's submarine cable database ([187]) – which provides details of all submarine cables that are planned, in deployment, operational or recently decommissioned worldwide, as of the second half of 2024 –,Axiom's expertise in the submarine cable industry and public announcements from submarine cable owners. Information from these sources has been validated against other third-party sources, such as the Submarine Telecoms Forum Almanac, ([188]) the ITU-T BB map, ([189]) Infrapedia ([190]) and TeleGeography, ([191]) to identify any conflicting information.

The mapping exercise presented herein has been conducted exclusively on the basis of publicly available sources, without reliance on sensitive information. The mapping was subsequently revised and validated by the Expert Group. The work conducted by the Contractor and the Expert Group has resulted in the development of a mapping tool that includes almost 300 submarine cables (which land in the EU or are of special relevance for the EU) and which was made available to Member States.

Based on analysis conducted by the Contractor using the mapping tool, the following colour codes are used to represent the status of each cable in the maps included in the remainder of this section:

- operational (green)
- some sections operational (dashed green)
- in deployment (dashed blue)
- planned (dashed grey)
- suspended (dashed red)
- decommissioned (red).

In addition, yellow is used to highlight a particular cable in the maps, regardless of its operational status.

([187]) Analysys Mason (2024), *Submarine cable database 1H 2025*.

([188]) Submarine Telecoms Forum (2025), *Submarine cable Almanac*.

([189]) ITU (2025), *Infrastructure Connectivity Map*.

([190]) Infrapedia (2025), *Submarine cable map*.

([191]) TeleGeography (2025), *Submarine Cable Map*.

4.2. Submarine data cable infrastructure in the EU

As described in Section 3.1, there are two main types of submarine cable infrastructures in Europe:

- cables connecting EU Member States to non-EU Member States, and
- cables interlinking EU Member States, including their outermost regions, overseas countries and territories (ORs and OCTs.

As of April 2025, there were 236 operational submarine cables landing on the European continent and the EU ORs. Of these, 200 cables had at least one landing station in an EU Member State, with the remaining cables landing in strategic non-EU countries such as the UK, Norway, Russia, Iceland, Georgia, Ukraine, Albania or Azerbaijan.

Out of the 200 cables with at least one landing station in an EU Member State:

- 100 cables provide international connectivity between EU Member States and non-EU countries
- 100 cables exclusively provide intra-EU connectivity (i.e., EU-to-EU Member States and Member States internal connections). ([192])

Throughout this section, unless explicitly stated otherwise, **capacity** refers to the maximum design capacity achievable with the current submarine cable technology. It should be noted that this capacity may have changed since the last publicly available data.

The capacity analysis presented across this section only includes repeated cables for Member States and the EU ORs:

- Unrepeated cables are typically intra-national or regional, designed to handle domestic traffic and complement terrestrial networks. ([193]) These submarine cables are generally not interconnected to international hubs and, therefore, do not contribute significantly to EU-wide security and resilience. In addition, the characteristics of most unrepeated cables are not public.

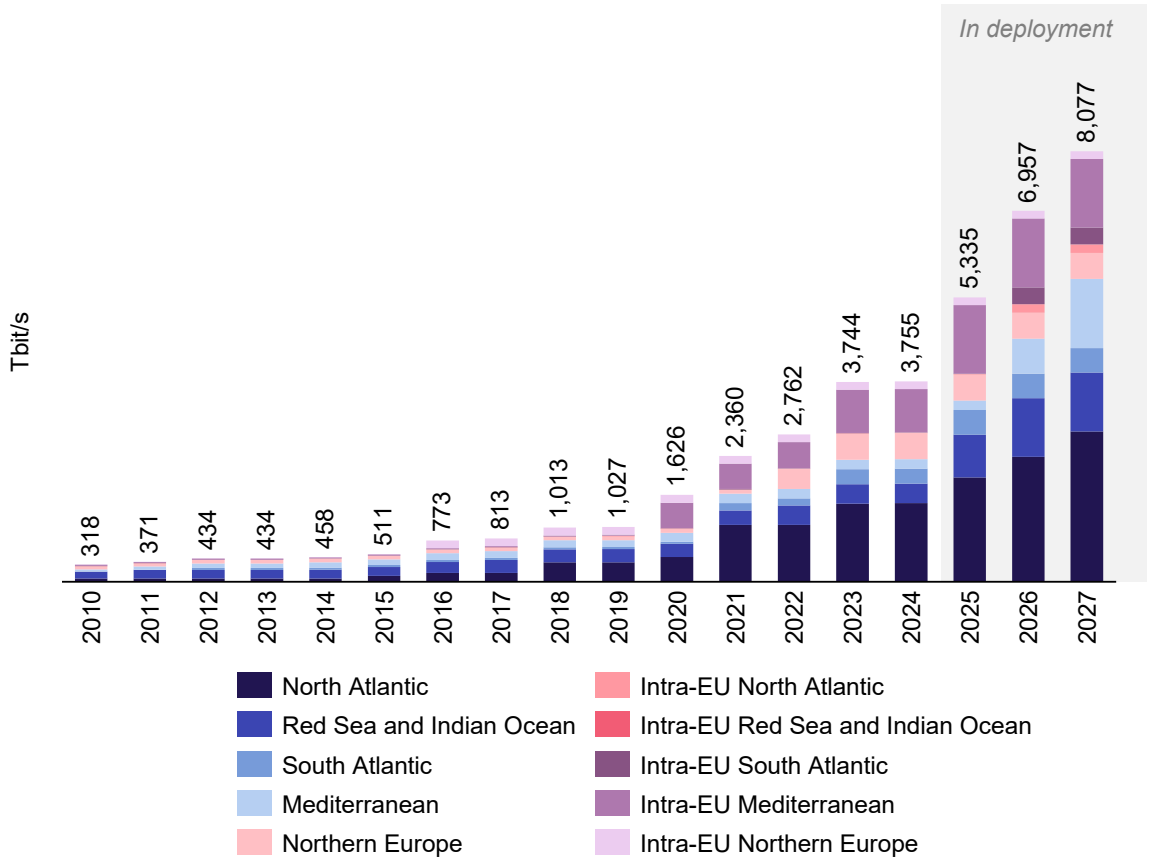
- Submarine cables connecting OCTs are also generally not interconnected to international hubs and, therefore, play a minor role in EU-wide security and resilience. However, these cables were qualitatively assessed in the route analysis for all defined geographical regions.

Total submarine cable capacity connecting the EU Member States between themselves and to outside countries increased from 318 Tbit/s in 2010 to 3755 Tbit/s in 2024, as shown in Figure 4.1.

([192]) This also includes cables in Greece, Spain and Portugal that connect islands within EU Member State territories.

([193]) Includes Olisipo, CrossChannel Fibre, IOEMA, Skagen Fibre West and Zeus.

Figure 4.1: Submarine cable capacity landing in at least one EU Member State [Source: Analysys Mason, 2025]



The growth in submarine cable capacity recorded over the past 10 years has mainly been driven by the rising demand for international capacity from the four-largest hyperscalers (Google, Meta, Microsoft and Amazon), which accounted for 71% of all used international capacity in 2024, up from 10% in 2014. ([194])

Although hyperscalers own the majority of submarine cable capacity on the transatlantic route, traditional operators and carriers own most of the capacity on other more regional routes. This is because the Middle East and North Africa (MENA) and Asia regions have historically seen limited investment in cloud services from hyperscalers, which have typically opted to lease managed capacity from traditional telecoms operators and carriers or acquire an IRU over a fibre pair on existing submarine cables. However, the landscape is evolving rapidly, and hyperscalers are now actively deploying submarine cables to connect this global infrastructure (for example, the Blue-Raman submarine cable, owned by Google as part of a consortium, or 2Africa, led by Meta), driven by the growing demand for cloud services ([195]) and data centres ([196]) in these regions.

A detailed capacity analysis for the different regions connecting EU Member States to the rest of the world is provided below. It is important to highlight that this analysis has been carried out using publicly available information. Therefore, the capacity of some of the submarine cables included in the analysis is unknown.

([194]) TeleGeography (2023), Submarine Cable Map 2023.

([195]) MENA Cloud Alliance (2023), *Cloud Competitiveness Index*.

([196]) Turner & Townsend (2024), *In-depth look at data centres in the Middle East.*

4.2.1. Submarine cables connecting EU Member States to non-EU countries

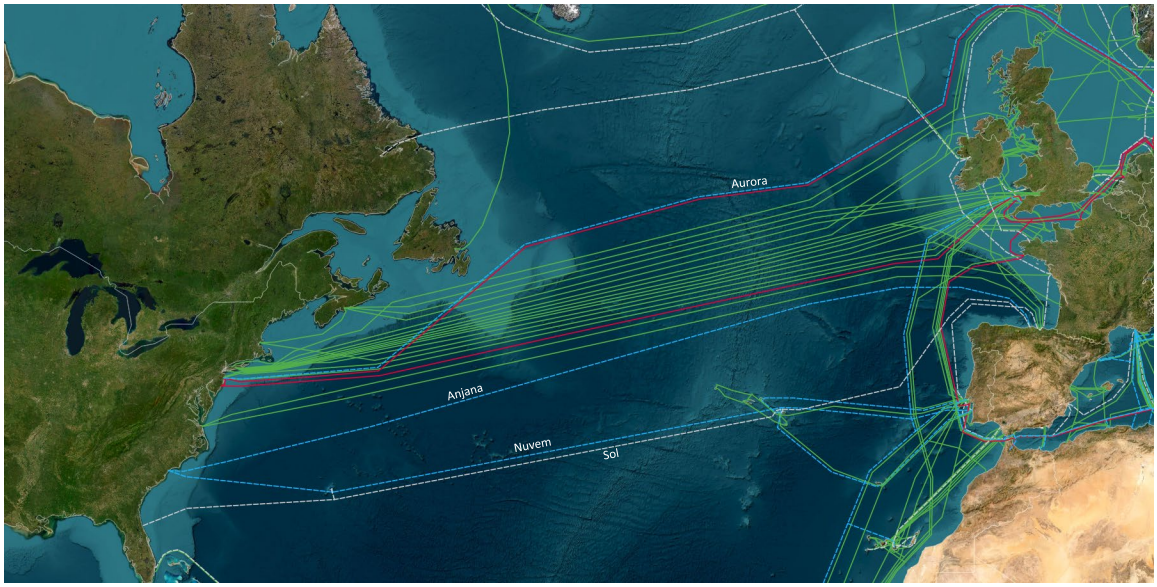
In this section, a deep analysis of the submarine cable infrastructures connecting EU Member States to non-EU countries has been carried out. The analysis is mainly focused on the total capacity on a per-region basis.

North Atlantic

The EU and North America are connected via 11 operational transatlantic cables, with a total capacity of 1450 Tbit/s, of which 1310 Tbit/s (90%) is owned by hyperscalers either as part of a consortium or through full ownership. Seven additional cables connect the EU ORs and OCTs in the North Atlantic, delivering a total capacity of 26 Tbit/s.

Total existing capacity for the North Atlantic region amounts to 1476 Tbit/s.

Figure 4.2: Submarine cables in the North Atlantic region [Source: Analysys Mason, 2025]

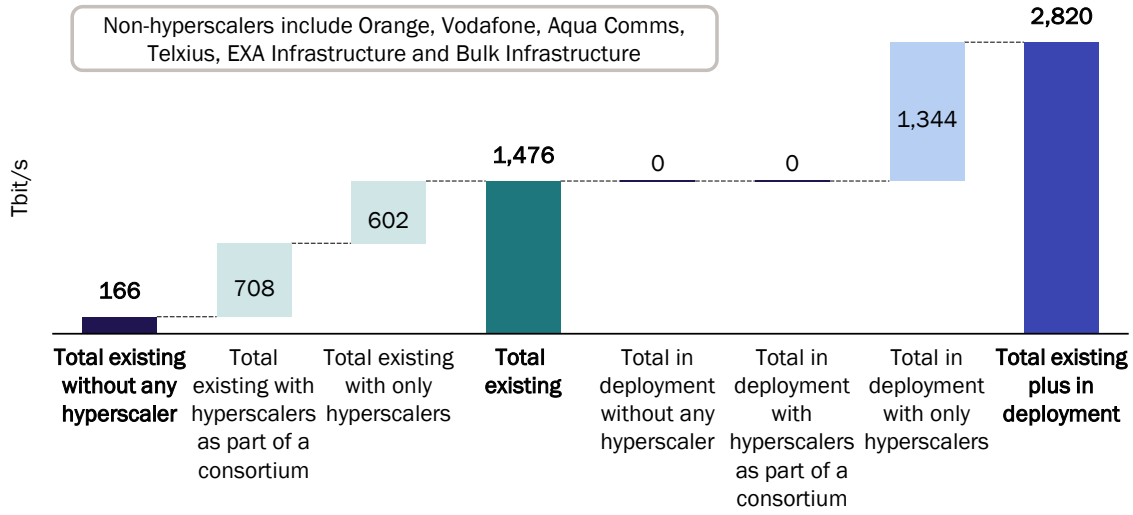


Three additional transatlantic submarine cables, which are currently in deployment, will almost double existing capacity in the near future. ([197])

These submarine cables will be fully owned by hyperscalers, meaning that, by 2027, hyperscalers will **own 94% of total capacity** in the North Atlantic region, as illustrated in Figure 4.3.

([197]) Anjana (a 480 Tbit/s cable owned by Meta), Nuvem (a 384 Tbit/s cable owned by Google) and Aurora (a 480 Tbit/s cable also owned by Meta).

Figure 4.3: Capacity of international submarine cables in the North Atlantic region [Source: Analysys Mason, 2025]



The dominance of hyperscalers on the transatlantic route is primarily driven by their need to interconnect US-based and European cloud regions (see Section 4.9). The amount of data transferred between different cloud regions is significantly higher than the data traffic handled by traditional telecoms operators, which explains the significant investments made by hyperscalers on the transatlantic route, compared to those made by telecoms operators.

Red Sea and Indian Ocean

Approximately 90% of the data traffic between Europe and Asia transits through the Red Sea ([198]) via eight different operational submarine cables, ([199]) which provide a total capacity of 316 Tbit/s. In addition, four cables are in deployment ([200]) on this route, which will more than double the existing capacity.

Furthermore, there are six operational cables connecting the EU ORs in the Indian Ocean (Réunion and Mayotte), with an aggregated capacity of 47 Tbit/s.

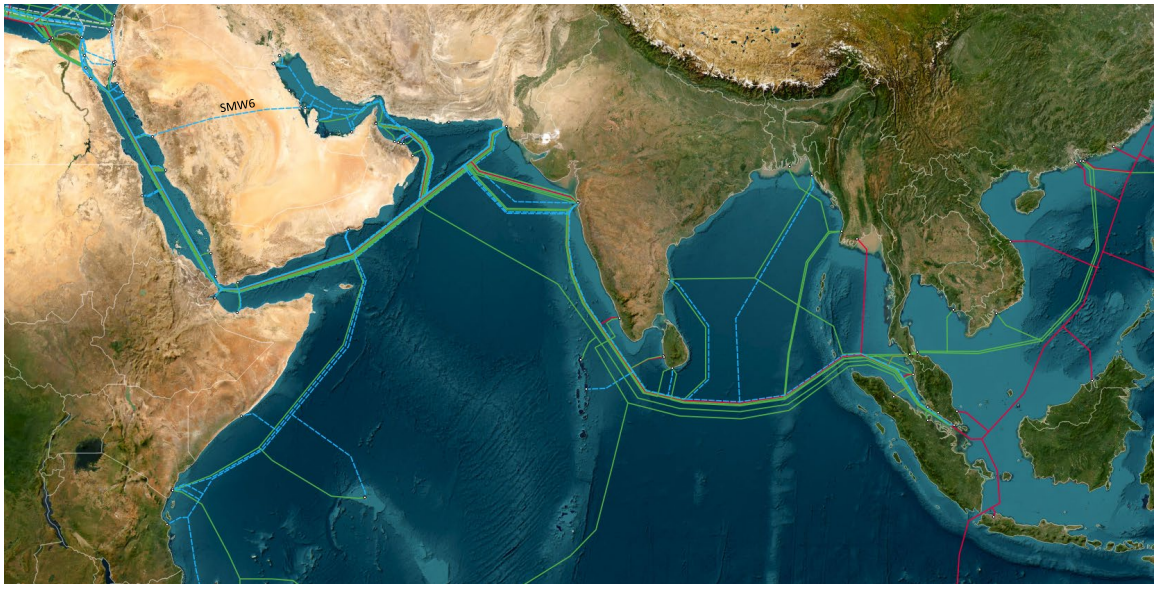
Total existing capacity in the Red Sea and Indian Ocean region amounts to 363 Tbit/s.

([198]) Centre for Strategic & International Studies (2024), *Red Sea Cable Damage Reveals Soft Underbelly of Global Economy*.

([199]) Asia Africa Europe-1 (AAE-1), Europe India Gateway (EIG), SEA-ME-WE 5 (SMW5), Middle East North Africa Submarine Cable System (MENA-SC), India-Middle East-Western Europe (IMEWE), FLAG Europe Asia (FEA), Pakistan and East Africa Connecting Europe (PEACE) and SEA-ME-WE 4 (SMW4).

([200]) Blue-Raman Submarine Cable System, India-Europe-Xpress (IEX), SEA-ME-WE 6 (SMW6) and Africa-1.

Figure 4.4: Submarine cables in the Red Sea and Indian Occean region [Source: Analysys Mason, 2025]



The Red Sea route is essential for communications between Europe and Asia. However, at the time of writing this report, it is challenging to install and maintain submarine cables on this route, especially in the Gulf of Aden (Bab El-Mandeb Strait), due to the ongoing Israeli–Palestinian conflict.

If this situation persists, potential investors may be discouraged from investing in submarine cable projects in the region, which will be highly detrimental to Europe. As an example, the latest submarine cable planned by Meta, known as the Waterworth cable, will be routed from the east coast of the US to South Africa, India, Australia and back to the US west coast, bypassing Europe altogether.

The continuous increase in bandwidth demand between Europe and Asia is leading to a situation in which the existing capacity routed through the Red Sea is expected to be fully utilised, and the incremental traffic will need to be sent through alternative routes. There are currently four potential alternative routes to bypass the Bab El-Mandeb Strait:

- **Option 1** – this option is being considered for SMW6 to avoid the Bab El-Mandeb Strait and connect Europe to Asia via Saudi Arabia's terrestrial infrastructure to reach the Persian Gulf. This new route would create additional dependencies on Saudi Arabia.
- **Option 2** – this option is being explored by large-capacity projects such as 2Africa, ([201]) a submarine cable connecting 33 countries in emerging Asia–Pacific, MENA, sub-Saharan Africa and Western Europe. The 2Africa cable is already in deployment, and is expected to be the longest submarine cable in the world, spanning approximately 45 000 km. Although this option would avoid the Bab El-Mandeb Strait, it would significantly increase latency between Europe and Asia, which would have an adverse impact on end-user experience for real-time services (such as voice) as well as financial transactional services.
- **Option 3** – this option involves connecting to Asia via the US by using the extensive transatlantic and transpacific capacity. This, however, would increase latency between Europe and Asia and increase reliance on the US.

([201]) This system also has a branch connecting the Mediterranean region through the Red Sea.

- **Option 4** – this option consists of establishing a connection from northern Europe to Japan via the Arctic Pole and the Bering Strait, which would significantly reduce the length of the route and therefore improve latency and quality of service for end users. However, it faces substantial operational and political challenges:
    - to lay a cable through the Artic Pole, large icebreakers would need to be deployed to break the ice ahead of the cable laying vessel, which would be extremely costly
    - the Artic Pole accounts for nearly 20% of Russia's GDP ([202]) and is perceived by Russia as a strategic military area for NATO and its allies – a perception that has become even more topical in the context of the Russia–Ukraine conflict, and Finland and Sweden's accession to NATO ([203])
    - additionally, the Bering Strait is a bottleneck connecting the Artic Sea and the Bering Sea; these are shallow water environments and areas of intensive commercial transit and fishing activities, thus increasing the risk of submarine cables being accidentally damaged by human activity (through anchoring and fishing equipment, for instance).

As of July 2025, the capacity on the Red Sea route was solely owned by telecoms operators that need to connect to Europe. It should be noted that Chinese operators such as China Unicom, China Mobile and China Telecom are members of the consortium deploying the SEA-ME-WE 5 (SMW5) and Asia-Africa-Europe 1 (AAE-1) submarine cables, and these operators will soon increase their capacity ownership with India-Europe-Xpress (IEX), a 200 Tbit/s submarine cable connecting Mumbai (India) to Europe. Also, Hengtong Group (owner of HMNTech) has deployed the Pakistan and East Africa Connecting Europe (PEACE) cable, a privately owned 15 000 km submarine cable connecting Marseille (France) to Mumbai (India). Other operators owning capacity on this route include Reliance Jio, Telecom Egypt, Mobily, MTN, Bharti Airtel, Pakistan Telecom, e& (formerly Etisalat), Orange and Djibouti Telecom, among others.

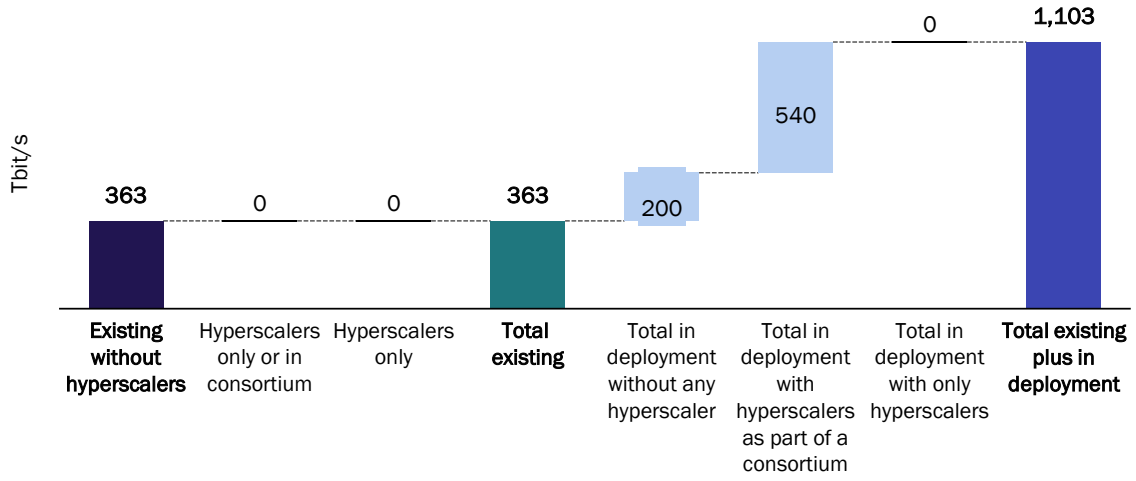
The new cables being installed will more than double the current total capacity, as illustrated in Figure 4.5 below. Hyperscalers do not currently own any capacity on these routes due to their underdeveloped cloud region infrastructure in the Middle East and Asia. However, with three large-capacity cables ([204]) in deployment, they will soon have access to significant capacity (540 Tbit/s) through their respective consortia.

([202]) Centre for International Maritime Security (2015), *Russia in the Arctic: Aggressive or Cooperative?*.

([203]) Chatman House (2025), *The militarization of Russian polar politics*.

([204]) Blue-Raman (Google and TI Sparkle), SWM6 (Microsoft and historical operators) and IEX (Meta, CMI and Jio reliance).

Figure 4.5: Capacity of international submarine cables in the Red Sea and Indian Ocean region [Source: Analysys Mason, 2025]



South Atlantic

The South Atlantic region also has a high presence of submarine cables, mainly connecting EU Member States in Western Europe (i.e., Portugal and Spain) with west and south African countries.

There are a total of seven cables connecting Africa to Europe, including state-of-the art cables such as Google's Equiano and EllaLink (the only cable linking the EU to South America), as well as older cables such the West Africa Cable System (WACS), Africa Cost to Europe (ACE), CanaLink, MainOne, and the South Atlantic Telecommunications cable no.3/West Africa Submarine Cable (SAT-3/WASC), with a total capacity of 281 Tbit/s.

Similar to the Red Sea and Indian Ocean region, up until 2023, submarine cable capacity along the western and southern Africa route was fully owned by historical operators such as Telkom, Orange, Angola Telecom, Telecom Namibia, AT&T, Portugal Telecom (currently Altice Portugal) and Deutsche Telecom. Again, the absence of private cloud regions in Africa up until recently explains the lack of hyperscale investment; it is understood that hyperscalers have historically leased managed capacity and swapped fibre pairs with other operators (such as Orange) on this route.

However, Google's Equiano cable, launched in 2023, has a total capacity of 144 Tbit/s, doubling the capacity on the African route, while 2Africa, led by Meta and with a capacity of up to 180 Tbit/s, will further increase capacity by more than 60% along this route by 2026 (see Figure 4.7).

Further, it is important to note that many African countries (Sierra Leone, Liberia, Guinea Bissau and Guinea) are directly connected via a single submarine cable (ACE). It should also be noted that, following a landslide on the Ivory Coast in March 2024, four ([205]) of the seven cables connecting West Africa were damaged, causing significant disruption to internet connectivity in these countries due to the lack of redundancy.

([205]) ACE, SAT-3, WACS and MainOne.

Figure 4.6: Submarine cables in the South Atlantic region [Source: Analysys Mason, 2025]

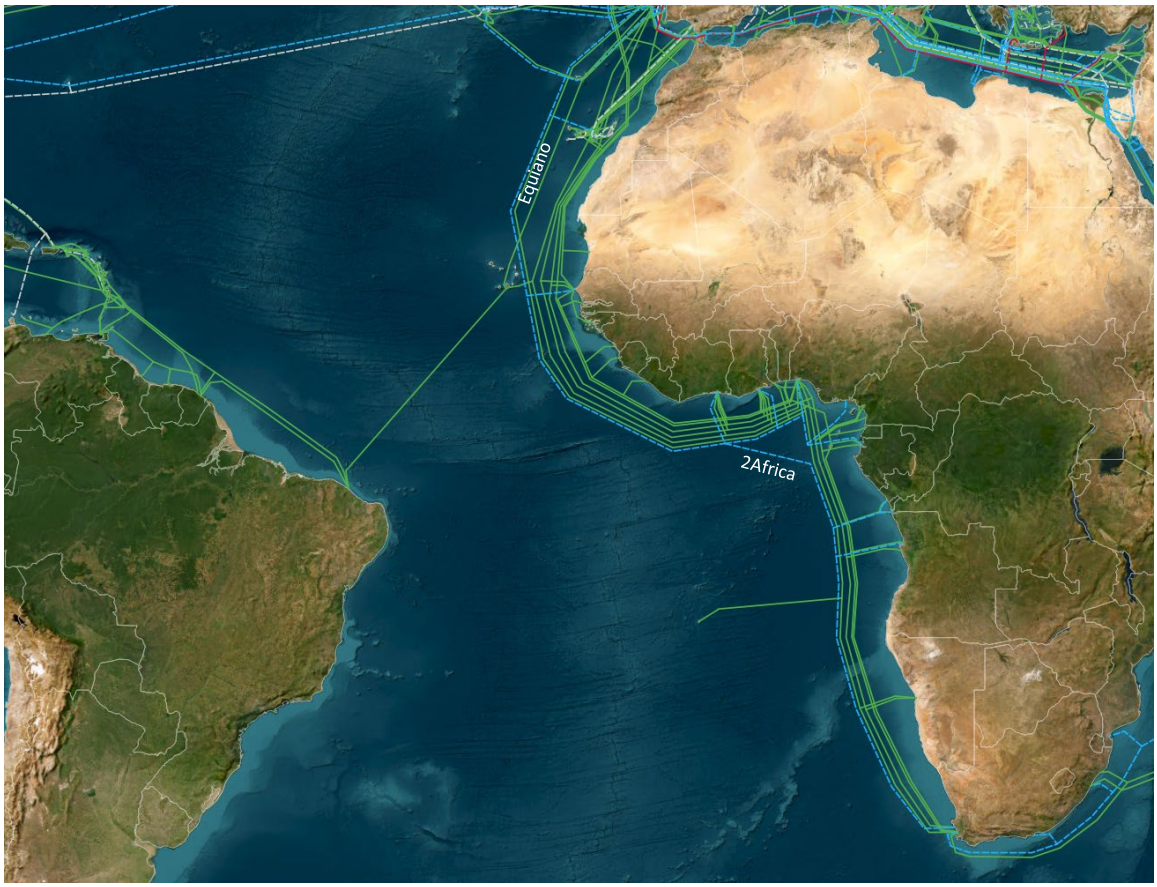
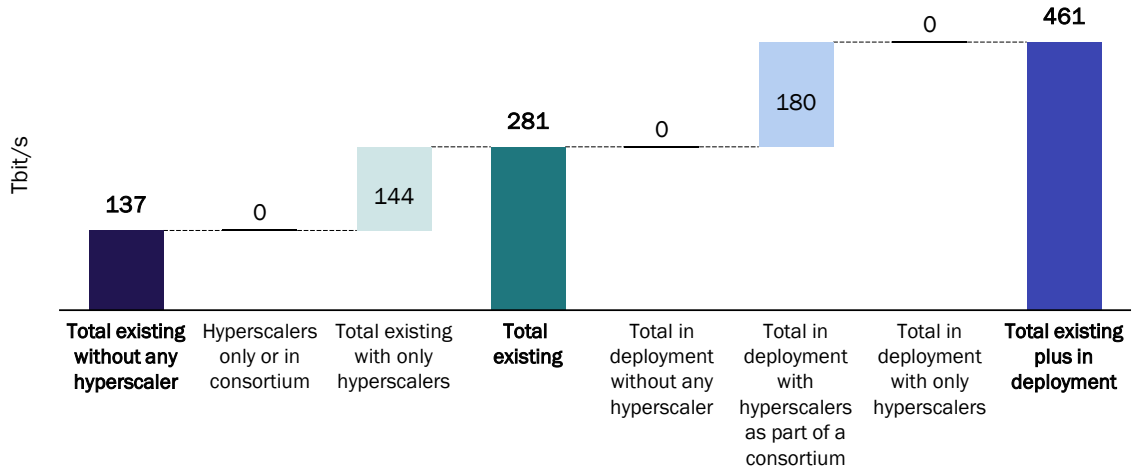


Figure 4.7: Capacity of international submarine cables in the South Atlantic region [Source: Analysys Mason, 2025]

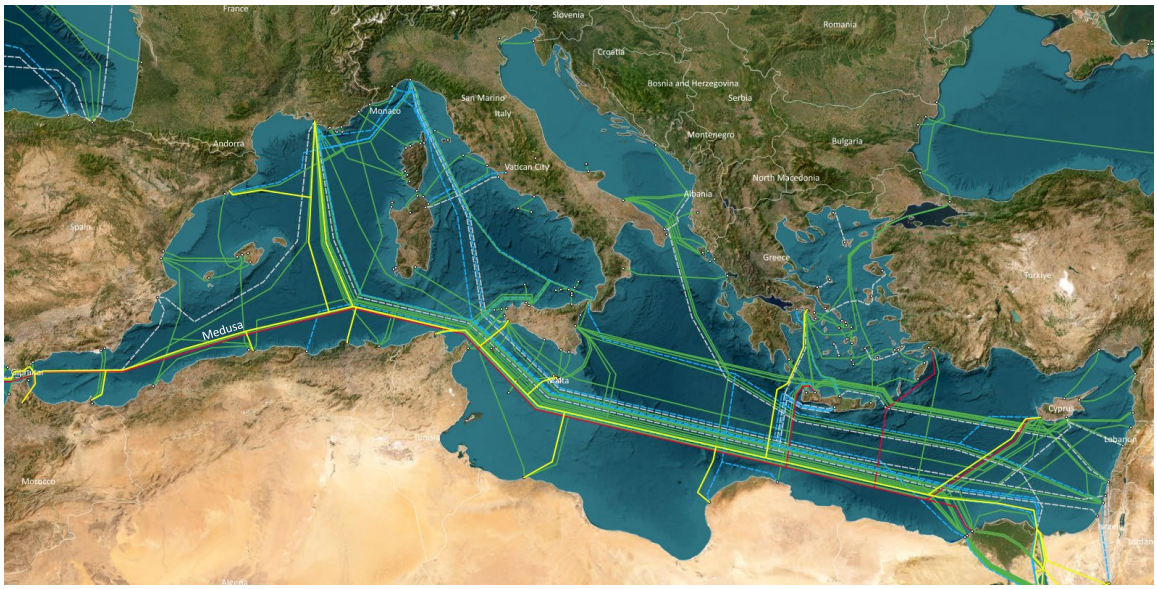


Mediterranean Sea

There are a total of 30 submarine cables interconnecting Southern Europe to Northern Africa and West Asia across the Mediterranean Sea, with a total capacity of 177 Tbit/s. ([206])

Given the more regional nature of the Mediterranean Sea, telecoms operators and carriers such as Cyta (Cyprus), Algeria Telecom (Algeria), Orange (France), Turk Telecom (Türkiye), Bezeq Telecom (Israel), Telecom Egypt (Egypt), Ooredoo (Qatar) and Telecom Italia (Sparkle, Italy) own the infrastructure.

Figure 4.8: Submarine cables in the Mediterranean region [Source: Analysys Mason, 2025]



Importantly, the **Medusa** ([207]) submarine cable, a EUR 342 million project strongly supported by the EU and the EIB, is a highly strategic project for the EU. Medusa will interconnect Portugal, Spain, France, Italy, Greece, Cyprus, Morocco, Algeria, Tunisia, Libya and Egypt through 21 landing points. Owned by Orange and AFR-IX telecom, the section of the Medusa cable connecting France to Morocco and Tunisia is expected to be RFS in 2026 . ([208]) With its 480 Tbit/s capacity, Medusa will quadruple existing capacity in the Mediterranean region, as shown in Figure 4.9.

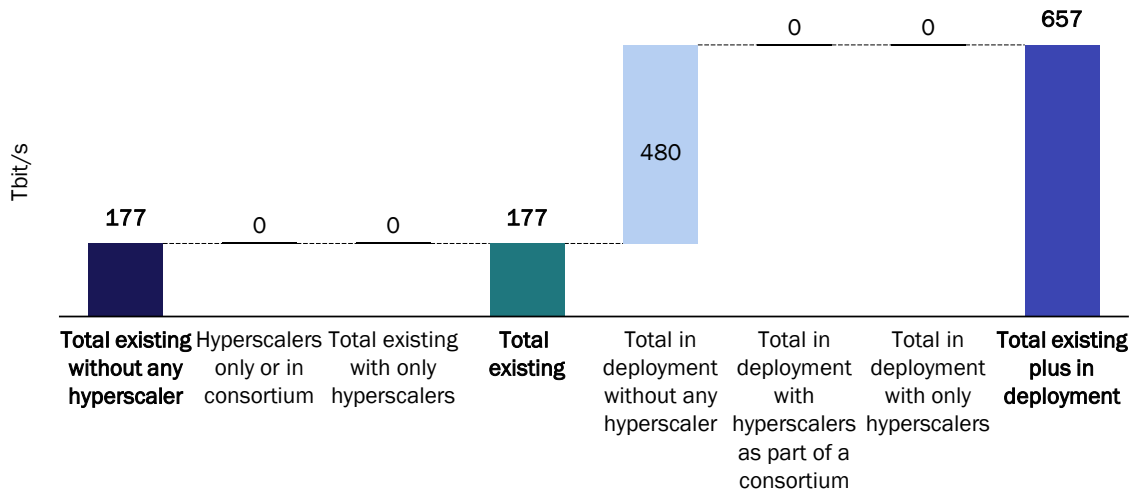
Hyperscalers own some capacity in the Mediterranean Sea through state-of-the-art cables connecting Europe to Asia and Africa (for example, 2Africa and IEX), as the Mediterranean Sea acts as a gateway to connect to other regions in the world. As noted before, however, these submarine cables have been included in the analysis of the Red Sea and Indian Ocean region.

([206]) Submarine cables linking the EU to southeast Asia through the Mediterranean Sea and the Red Sea are excluded from this analysis, as they are already considered within the scope of the Red Sea and Indian Ocean region, to avoid duplication.

([207]) AFR-IX telecom (2024), *The EU expands funding for Medusa with new grants*.

([208]) Connections to Greece, Libya, Cyprus and Egypt are still under discussion in terms of funding.

Figure 4.9: Capacity of international submarine cables in the Mediterranean region [Source: Analysys Mason, 2025]



Northern Europe

The Northern Europe region, comprising the Irish, Baltic and North Seas, and the English Channel, is linked via 32 submarine cables, with a total capacity of 486 Tbit/s. Seven cables provide 90% of the capacity: Havhingsten, IRIS, DANICE, ESAT-2, High-capacity Undersea Guernsey Optical Fibre (HUGO), Geo-Eirgrid and TGN Western Europe, with the Havhingsten cable accounting for more than 60% of total capacity in the region.

Havhingsten is a 300 Tbit/s submarine cable owned by a consortium led by Meta. It connects Denmark, the UK and Ireland, and is the largest capacity cable in Northern Europe. The cable connects Meta's cloud regions in Copenhagen (via terrestrial backhaul), Groningen (the Netherlands) and Amsterdam (the Netherlands).

Other than Meta, capacity owners include traditional operators such as Farice (Iceland), BT (UK), Sure (UK), Vodafone (UK), Tata Communications (India), Virgin Media Business (UK), eir (Ireland), EirGrid (Ireland) and Zayo (US).

In addition to these submarine cables, there are six short (unrepeated) very-high-capacity cables connecting Norway to Europe (HAVSIL), the UK to France (CrossChannel Fibre), Norway to Denmark (Skagen Fiber West), the UK to the Netherlands (Zeus) and Ireland to the UK (CeltixConnect-1, or CC-1).

Figure 4.10: Submarine cables in the Northern Europe region [Source: Analysys Mason, 2025]

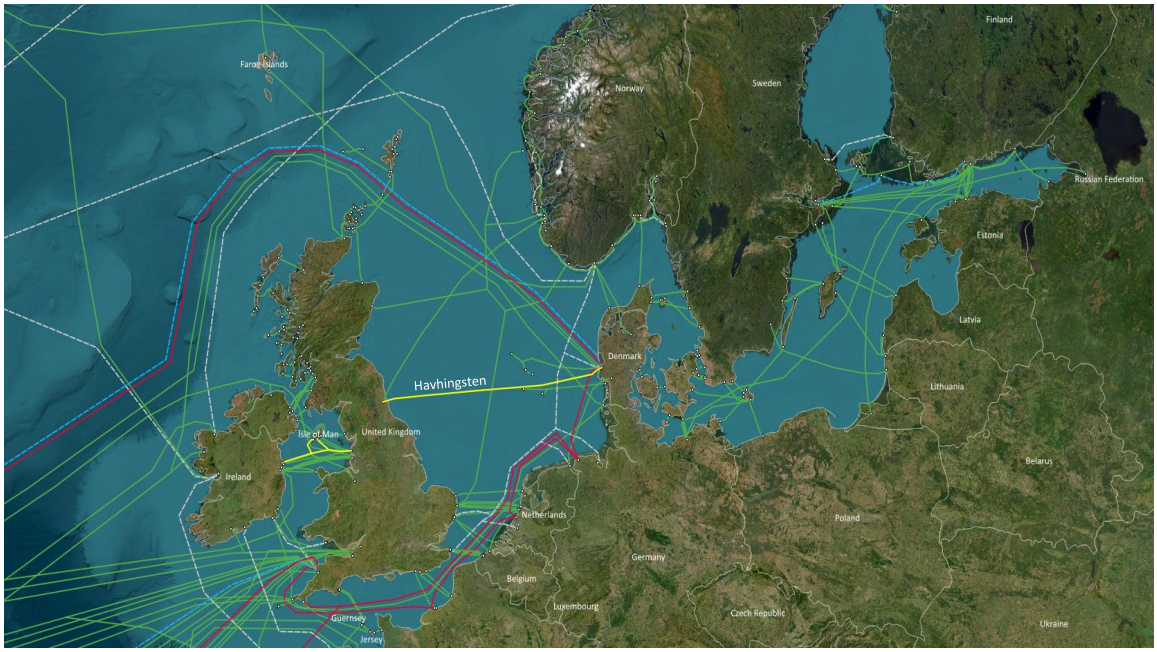
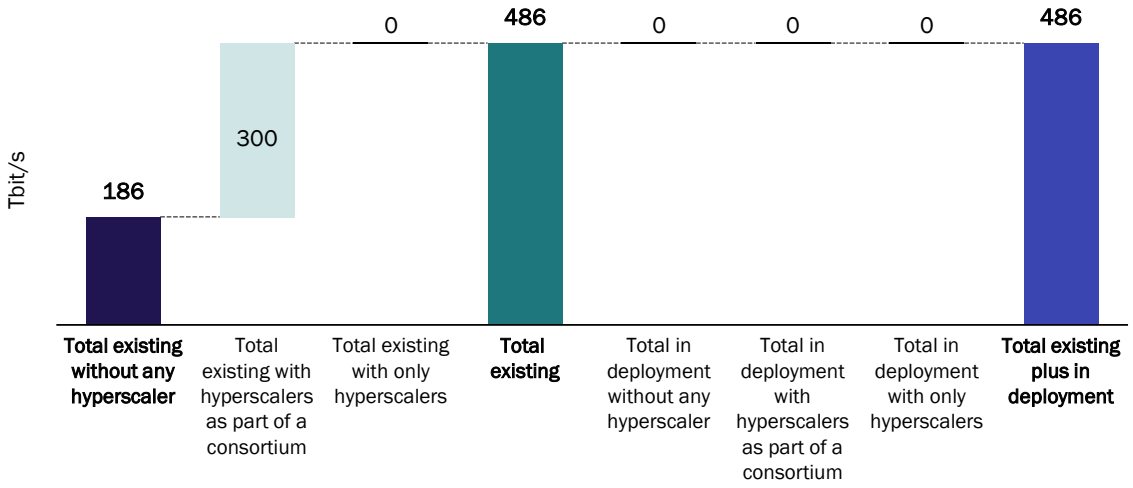


Figure 4.11 illustrates the total capacity of existing submarine cables in the Northern Europe region, connecting the EU to non-EU Member States.

Figure 4.11: Capacity of international submarine cables in the Northern Europe region [Source: Analysys Mason, 2025] ([209])



Finally, it should be noted that the Finish Ministry of Transport and Communications has tried to deploy cables through the Artic Circle, connecting Europe to Japan through the Bering Strait. However, as stated above, this cable route is extremely challenging from a political, environmental and operational point of view. Cross-polar projects such as the Artic Connect have already been attempted, but had to be suspended in 2021 "for further feasibility assessment". ([210])

([209]) The CC-1 submarine cable is excluded from Figure 5.11 because it is a point-to-point unrepeated cable (hence more comparable to terrestrial cables) and its large capacity would have introduced a bias in this study.

([210]) Submarine Cable Networks (2021), *Trans-Arctic cable project Arctic Connect comes to a suspension*.

More recently, the Polar Connect project, partly funded by the EU, is a Nordic initiative coordinated by Sweden that aims to deploy a submarine cable to connect Norway, Canada and Japan via the Artic Pole and the Bering Strait. To de-risk the project, seabed surveys were carried out successfully in the summer of 2025, with the RFS date planned for 2030. ([211]) It should be noted that an ice-breaking vessel has yet to be built by Sweden to accompany the vessel that will lay the cable. The Swedish Government has initiated a formal review to access cost-effective options for securing access to a new polar research icebreaker.

In February 2025, a European Consortium comprising Cinia Oy, NORDUnet A/S, Tusass A/S, the Dutch Subsea Cable Coalition, GlobalConnect AB and Tampnet AS signed an MoU to establish a Pan-Arctic Cable System (PACS) between Europe and Asia via the Arctic and North America. PACS signatories work together with Polar Connect to discuss synergies to insure Artic connectivity. ([212])

It should be noted that many other cables interconnecting EU countries exclusively (such as C-Lion1, which directly links Finland and Germany) are excluded from Figure 4.11, as they are included in the intra-EU Member States category, below.

4.2.2. Submarine cables interconnecting EU Member States

EU Member States are internally interconnected through 100 submarine cables, mainly located in the North/Baltic Sea and the Mediterranean Sea, while the ORs and OCTs in the Atlantic and Indian Ocean are also linked via submarine cables.

Intra-EU submarine cable capacity is solely owned by historical operators such as Orange (France), Telecom Italia and Telefónica (Spain), ([213]) as well as international carriers such as Global Connect (Sweden), AT&T (US), Verizon (US) and Colt (UK). Hyperscalers do not own any of this infrastructure and have no deployment plans to interconnect EU countries.

Similar to the previous section, an analysis of the submarine cables connecting EU Member States has been conducted with a focus on the total capacity by region.

Intra-EU North Atlantic

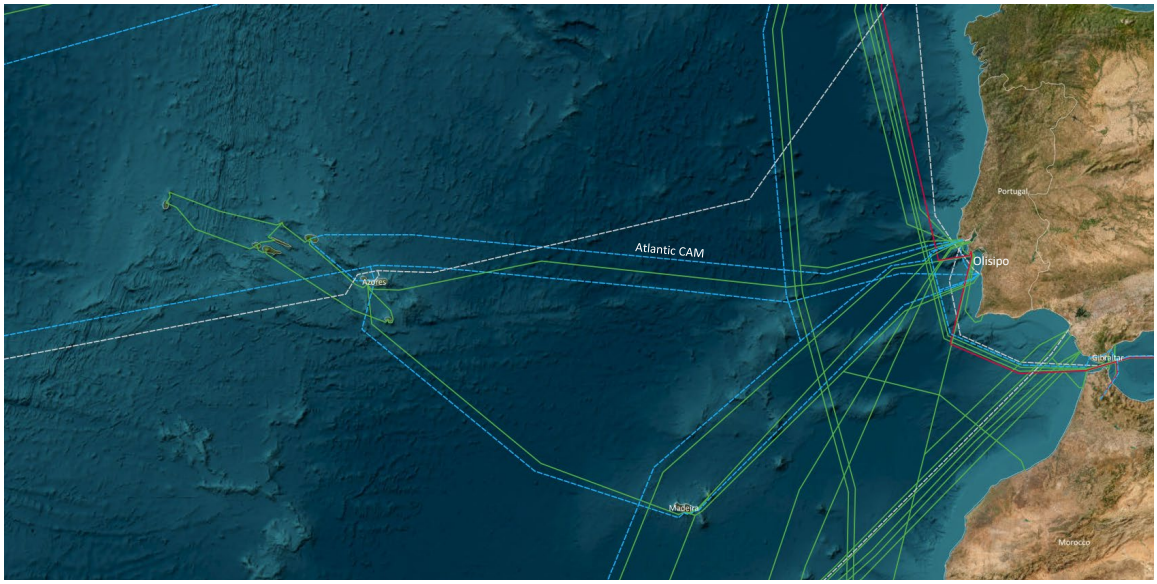
The Intra-EU North Atlantic region mainly comprises submarine cables connecting mainland Portugal to its ORs Azores and Madeira, as well as a cable connecting French Guiana to Martinique (French ORs).

([211]) EMEA Submarine Networks Conference 2025, News brief Polar Connect, 18 February 2025.

([212]) NORDUnet (2025), *NORDUnet signs MoU with partners in Pan-Arctic subsea cable collaboration*.

([213]) Although Telefónica is referenced throughout this document, it should be noted that submarine cables landing outside Spain are owned and operated by Telxius, a subsidiary of Telefónica Infra.

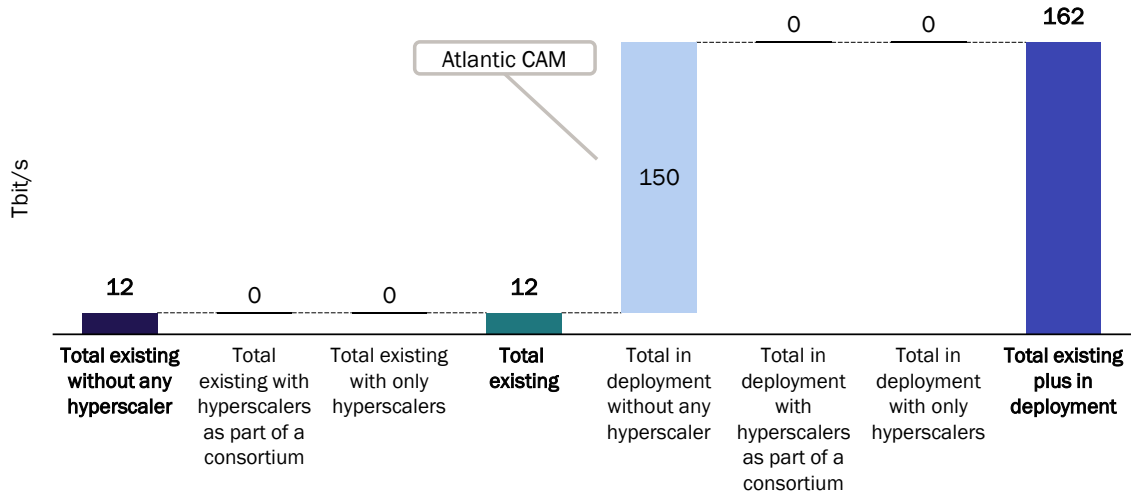
Figure 4.12: Submarine cables in the Intra-EU North Atlantic region [Source: Analysys Mason, 2025]



These cables have a total capacity of 12 Tbit/s and are solely owned by telecoms operators such as Altice Portugal, Orange (France), AT&T (US) and Verizon (US).

In addition, there are two submarine cable in deployment (Atlantic CAM and Olisipo), which are expected to be RFS by 2026.

Figure 4.13: Capacity of submarine cables interconnecting EU Member States in the Intra-EU North Atlantic region [Source: Analysys Mason, 2025] ([214])



([214]) Olisipo has been excluded from this capacity analysis, as it is an intra-national unrepeated cable which complements the national terrestrial network.

Intra-EU Red Sea and Indian Ocean

At the time of writing this report, there are no submarine cables interconnecting EU Member States in the Intra-EU Red Sea and Indian Ocean region. The ORs in the Indian Ocean (i.e., Mayotte and Réunion) are connected to other countries via submarine cables and have already been considered within the Red Sea and Indian Ocean region.

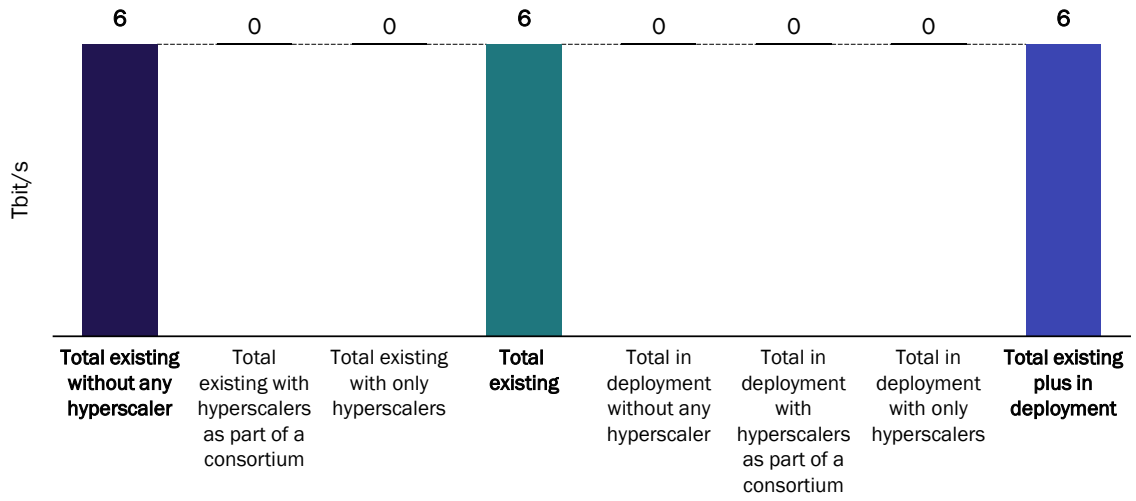
Intra-EU South Atlantic

The Intra-EU South Atlantic region predominantly encompasses submarine cables connecting mainland Spain to its outermost region, the Canary Islands, in addition to submarine cables interlinking these islands.

Figure 4.14: Submarine cables in the Intra-EU South Atlantic region [Source: Analysys Mason, 2025]

These cables have a total capacity of 6 Tbit/s and are wholly owned by Canalink (Spain) and Telefónica (Spain).

Figure 4.15: Capacity of submarine cables interconnecting EU Member States in the Intra-EU South Atlantic region [Source: Analysys Mason, 2025]



Intra-EU Mediterranean

This region has the largest number of intra-EU submarine cables, 37 in total, with a total capacity of 811 Tbit/s. As with other intra-EU regions, the capacity on these cables is fully owned by historical operators such as Orange (France), Telecom Italia (Sparkle, Italy), Telefónica (Spain) and Vodafone (UK).

Figure 4.16: Submarine cables in the Intra-EU Mediterranean region [Source: Analysys Mason, 2025]

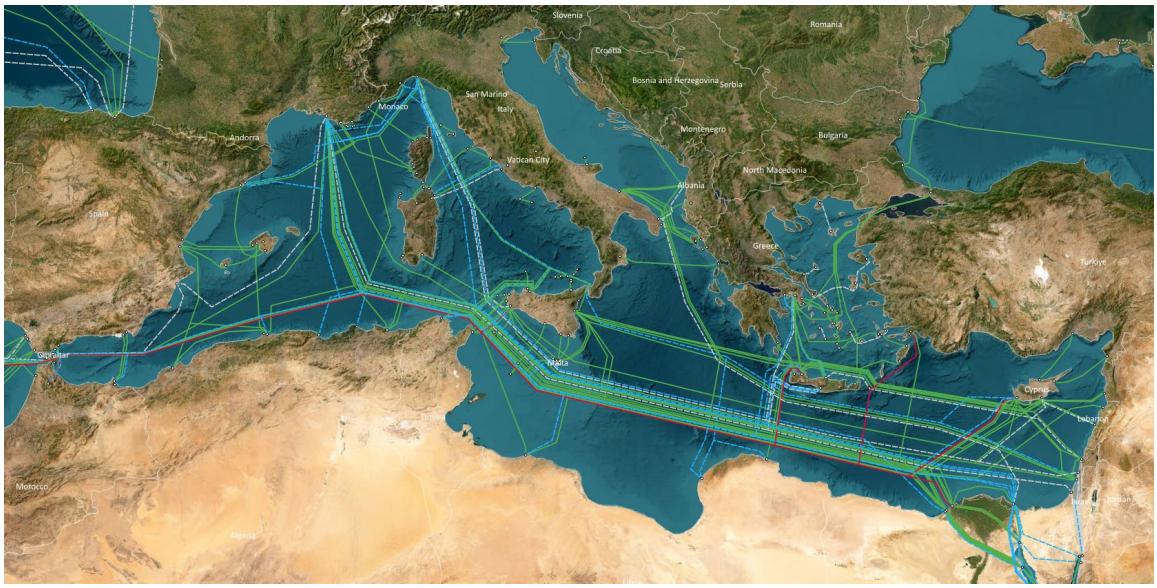
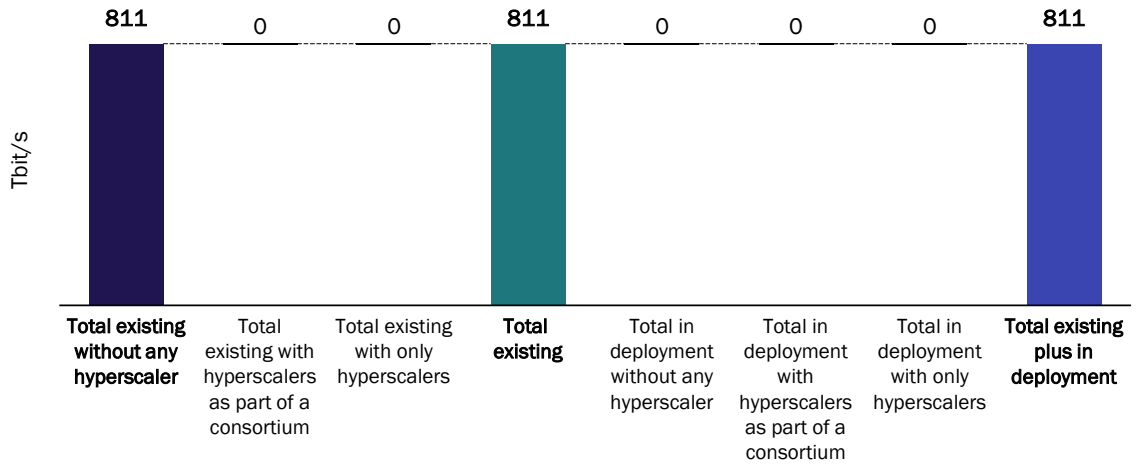


Figure 4.17: Capacity of submarine cables interconnecting EU Member States in the Intra-EU Mediterranean region [Source: Analysys Mason, 2025]



Intra-EU Northern Europe

This region comprises the Baltic Sea, the North Sea, the Irish Sea and the English Channel.

Submarine cables in this region have a known capacity of 144 Tbit/s, which is exclusively owned by operators such as Cinia (Finland), Colt (UK), Arelion (Sweden), GlobalConnect (Denmark), Telia (Sweden) and Telenor (Norway), with no presence of hyperscalers.

Most of the available capacity in this region is carried out by the C-Lion1 cable connecting Finland to Germany in the Baltic Sea. ([215])

Figure 4.18: Submarine cables in the Intra-EU Northern Europe region [Source: Analysys Mason, 2025]

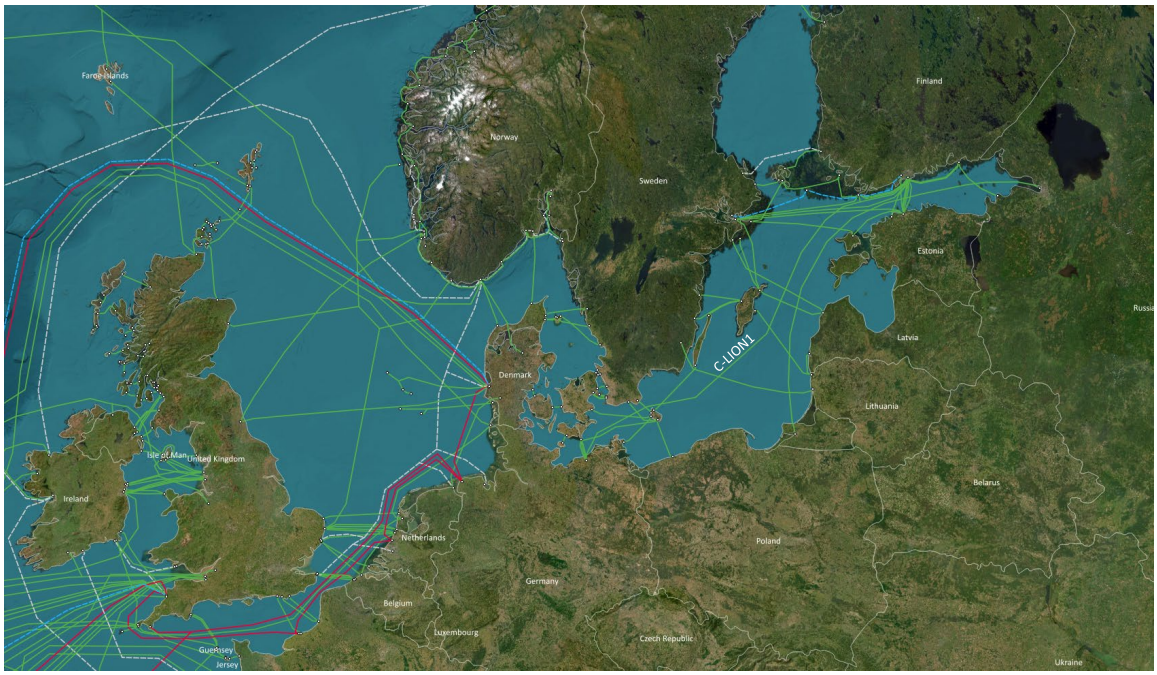
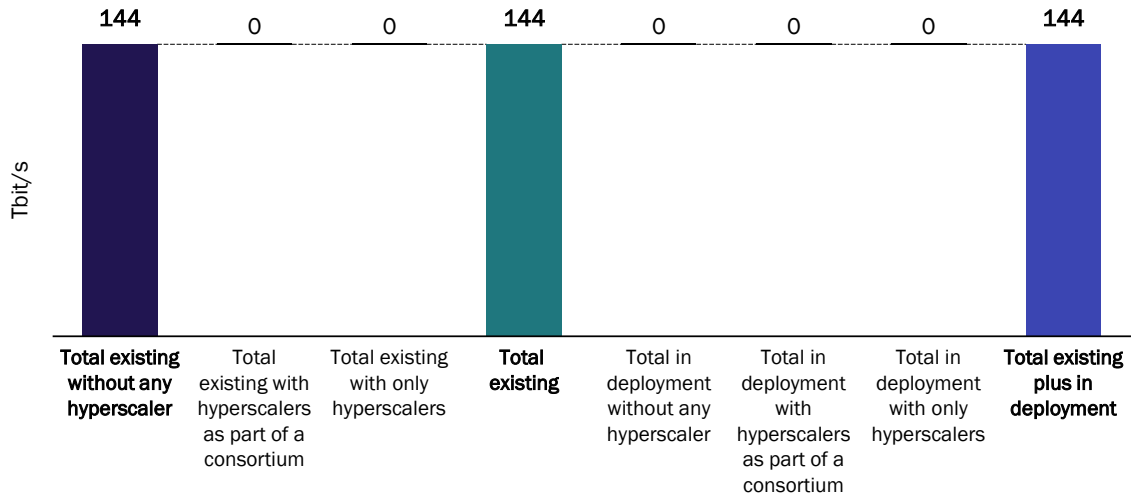


Figure 4.19: Capacity of submarine cables interconnecting EU Member States in the Intra-EU Northern Europe region ([215]) [Source: Analysys Mason, 2025]



4.3. Relevant submarine cable infrastructures connecting non-EU countries

An analysis of submarine cable capacity has been conducted for two non-EU countries (the UK and Norway), based on their relevance and geographical proximity to the EU. The following capacity analysis excludes submarine cables connecting the UK and Norway to EU Member States, as they have already been included in the previous section.

4.3.1. UK

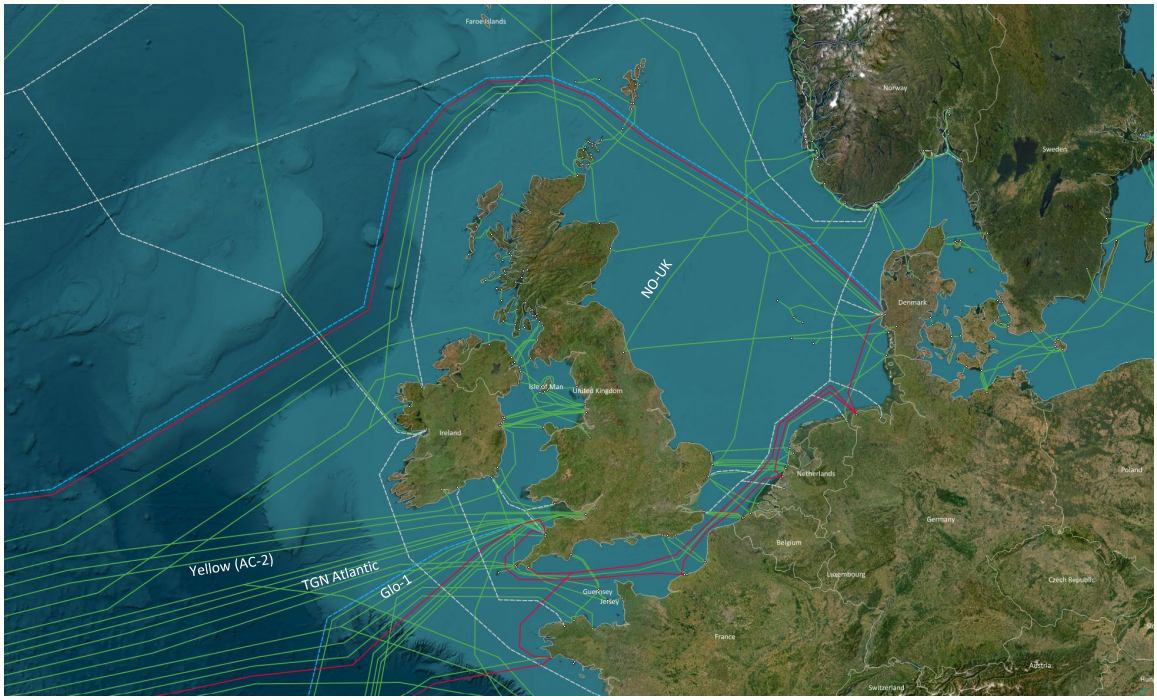
There are 25 submarine cables connecting the UK internally and to other countries. These cables are solely owned by operators such as BT (UK), Sure (UK) or Vodafone (UK).

There are five main submarine cables in the UK providing international connectivity: two transatlantic cables connecting the UK and the US (Yellow and TGN-Atlantic), two cables connecting the UK and Norway (NO-UK and Tampnet Offshore FOC Network), and one cable connecting the UK and Africa (Globacom-1 (Glo-1)).

In addition, two cables connect the UK to the Faroe Islands (FARICE-1 and SHEFA-2).

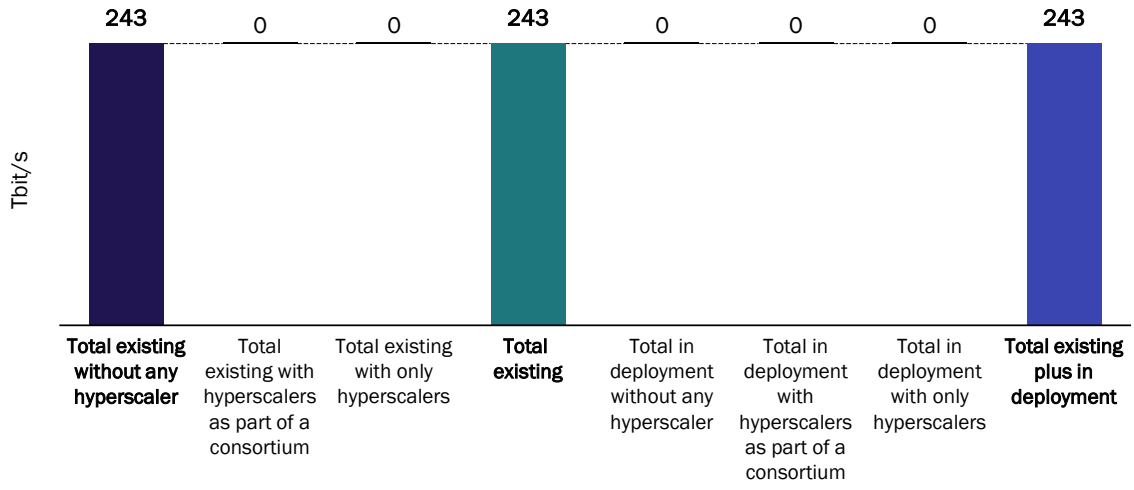
([215]) The 144 Tbit/s represents the C-Lion 1 capacity, as the capacity of other unrepeated cables in the region is not publicly available.

Figure 4.20: Submarine cables linking the UK to other countries [Source: Analysys Mason, 2025]



Total cable capacity amounts to 243 Tbit/s, with no hyperscaler presence. Most of the capacity is carried on the NO-UK cable (216 Tbit/s), linking the UK to Norway.

Figure 4.21: Capacity of additional submarine cables interconnecting the UK [Source: Analysys Mason, 2025]



It should be noted that the EU has historically relied on the UK to connect mainland Europe with Ireland, and to facilitate transatlantic communications. The UK has also served as a key landing point for US transatlantic cables, positioning it as a central hub for international data transmission.

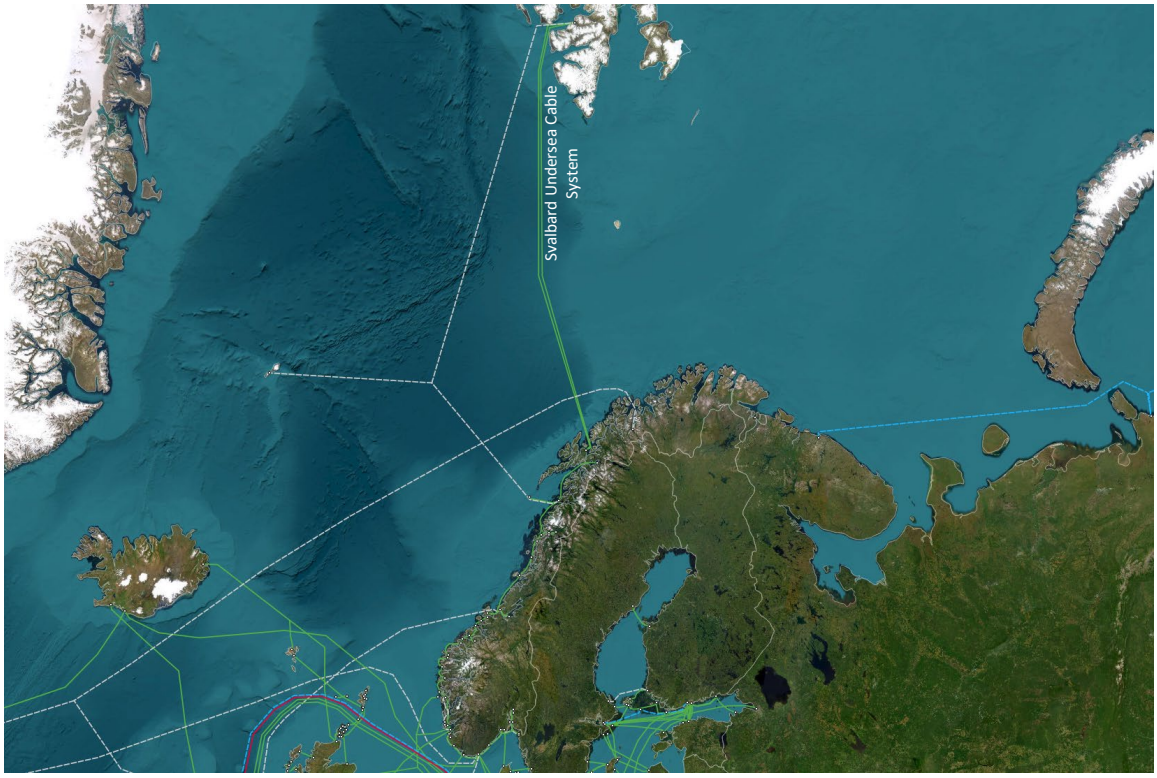
Ireland's connectivity to the EU is heavily dependent on submarine cables that often pass through the UK. Initiatives like the PISCES submarine cable aim to establish direct connections between Ireland and mainland Europe, reducing reliance on the UK. However, until these projects are fully operational, the UK remains a crucial intermediary for Ireland's digital connectivity.

4.3.2. Norway

Six submarine cables link different locations within Norway, with a total capacity of 5 Tbit/s. ([216]) These cables are wholly owned by Norwegian operators such as Space Norway, Telenor, Eviny Digital and KystTele.

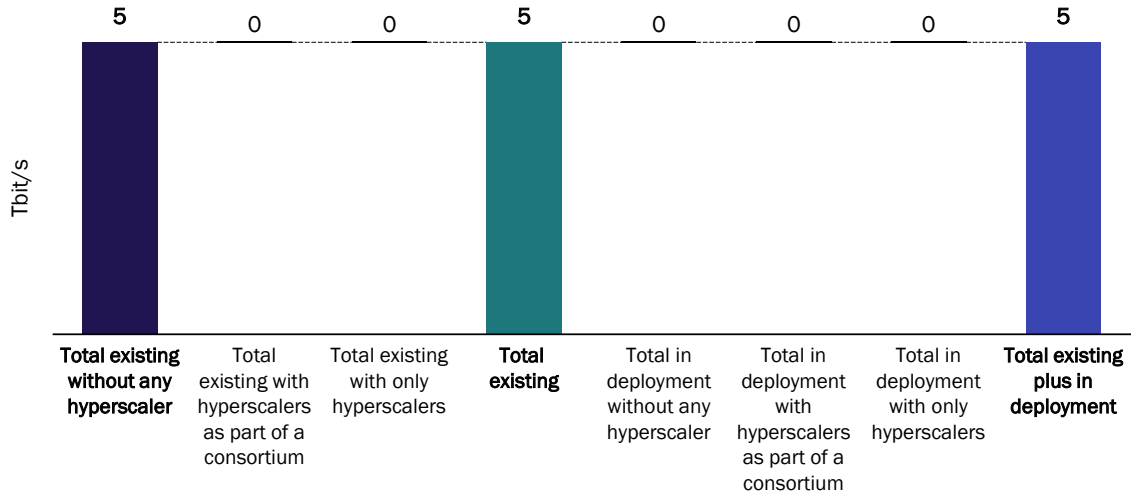
All of these submarine cables connect different locations within the country, and none of them provides international connectivity to other countries (except for the NO-UK cable, included in the analysis of submarine cable capacity for the UK, and the cables connecting Norway to EU Member States, as shown in the previous section).

Figure 4.22: Submarine cables providing domestic connectivity in Norway [Source: Analysys Mason, 2025]



([216]) Total capacity is publicly available only for one of the six submarine cables connecting Norway (the Svalbard Undersea Cable System).

Figure 4.23: Capacity of additional submarine cables connecting different locations within Norway [Source: Analysys Mason, 2025]



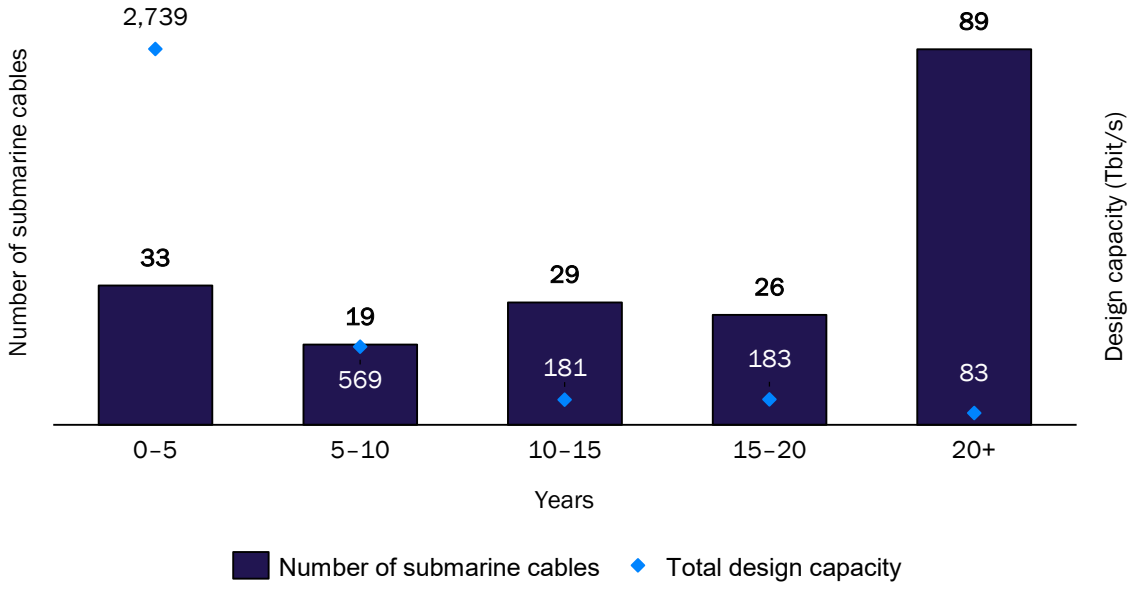
In addition, Bulk Infrastructure (Norway) plans to deploy a new transatlantic cable linking Norway to Canada by 2027, named Leif Erikson, but capacity details have not been disclosed.

4.4. End-of-life analysis

Submarine cables usually have a design life of 25 years, but it may potentially be extended if it proves economically viable. However, for most cables, their end-of-life is dictated by the deployment of the next generation of submarine cables, which eclipses the capacity of legacy cables and makes them uneconomical to run.

As shown in Figure 4.24, the 31 newest cables provide 74% of the total capacity currently provided by submarine cables landing in at least one EU Member State. In contrast, the 91 oldest cables represent only 2% of the total current capacity of submarine cables landing in at least one EU country. However, legacy submarine cables carry public telecoms traffic, unlike the new generation of cables owned by hyperscalers which are laid for their own private use. Therefore, when legacy cables reach their end-of-life, telecoms operators will need to secure some capacity on these newer cables to handle the rising demand for data traffic and ensure public service continuity.

Figure 4.24: Number of submarine cables landing in the EU, total capacity and age [Source: Analysys Mason, 2025] ([217])



4.5. Planned cables

As of July 2025, a total of 23 new submarine cables with at least one landing station in the EU are planned. ([218]) However, it should be noted that these cables have not been included as part of the previous capacity assessment due to the uncertainty surrounding these planned deployments.

Large international connectivity cables such as CADMOS-2, Celtic Norse, the East to Med Corridor (EMC) West, Far North Fiber, Pan-Arctic Cable System (PACS) and EAGLE are still in their planning phase. As a result, information on the available capacity of these upcoming cables is largely unavailable at this stage.

Future deployments are aimed to increase redundancy on the North Atlantic, Mediterranean and Red Sea routes, with a few additional new cables providing connectivity between EU Member States, as shown in Figure 4.25.

([217]) Three submarine cables landing in the EU have been excluded from this analysis (CrossChannel Fibre and Skagen Fiber West, and Zeus, which connect the EU to the UK and Norway, respectively) due to their special characteristics and large capacity.

([218]) 'Planned' means that the cable is still being discussed by various stakeholders and that no formal contract has yet been executed.

Figure 4.25: Planned submarine cables in Europe [Source: Analysys Mason, 2025]

In addition to the cables shown in Figure 4.25, there are other submarine cable projects which have already received funding from the CEF programme, ([219]) but are still at a very early stage (i.e., initial feasibility study). These cables include the Myanmar/Malaysia India Singapore Transit (MIST) cable, the Magna Grecia cable, GreenMed, Stockholm Backbone, the Northern EU Gateways project, the Bonaire and Curaçao Submarine Cable (BCA), Canary Subsea STD, Madeira Connection, FII and the West European Coast Festoon (WECF) project.

4.6. Fault analysis

The time to repair submarine cable faults is increasing globally, ([220]) as stated by the Submarine Telecoms Forum in its Industry report 2024–2025. ([221])

As mentioned in Section 3.3.2, repairing a submarine cable involves identifying the fault location, obtaining the operational permit (if required), preparing the vessel with spares, cable and crew, travelling to the repair location and repairing the cable.

In large basins such as the Atlantic and the Mediterranean Sea, for repeated cables, it typically takes 24 hours to load the spares and prepare the crew, followed by 1 to 5 days of travel to the fault location, and an additional 5 to 10 days to repair the fault and test the cable, resulting in total duration ranging from 7 to 20 days on average.

In smaller basins where unrepeated cables are prominent (for example, the Baltic Sea), maintenance vessels and depots are generally located closer to the fault location, which helps to reduce transit time. Additionally, unrepeated cables are simpler to repair tan repeated cables because they do not require power. As a result, it typically takes 24 hours to load the spares and

([219]) European Commission (2024), *New projects signed under CEF Digital to enhance and strengthen submarine cable infrastructure across and to the EU*.

([220]) The global number of faults is driven by the number of faults in Asia where it is increasingly challenging to obtain permits which significantly drives the faults repair time up in this region.

([221]) Submarine Telecoms Forum (2025), *Industry report 2024–2025*.

prepare the crew, 1 day of travel to the fault location, and 3 to 5 days to repair the fault and test the cable, leading to an overall duration of 4 to 6 days on average.

It is worth noting that the replacement of submerged equipment such as repeaters, ROADM or branching units increases the repair duration by 3 to 6 days on average.

However, severe weather events may extend this timeline by several weeks, as the vessels cannot travel to the repair location. As a worst-case example, a cable repair in the middle of the North Atlantic in 2018 took 5 months (instead of the 3 weeks initially estimated) due to a succession of events, including a hurricane, which caused damage to the vessel foredeck while transiting to the repair site, difficulties in recovering the cable, a diversion to assist another vessel, and adverse weather conditions that forced the vessel to abandon the site. ([222])

To assess whether the existing maintenance fleet serving Europe is adequate to handle the growing volume of faults, two primary factors need to be considered:

- the evolution of the total number of faults by European region, and
- how often a vessel was unavailable for immediate deployment due to being engaged in repairing another cable.

Each of these factors is discussed in turn below. It should be noted that increasing the number of maintenance vessels would not reduce permitting delays.

4.6.1. Analysis of fault volumes in Europe

To assess how the number of submarine cable faults has evolved over time across the different European regions, the analysis considers faults within the geographical areas covered by the following maintenance agreements:

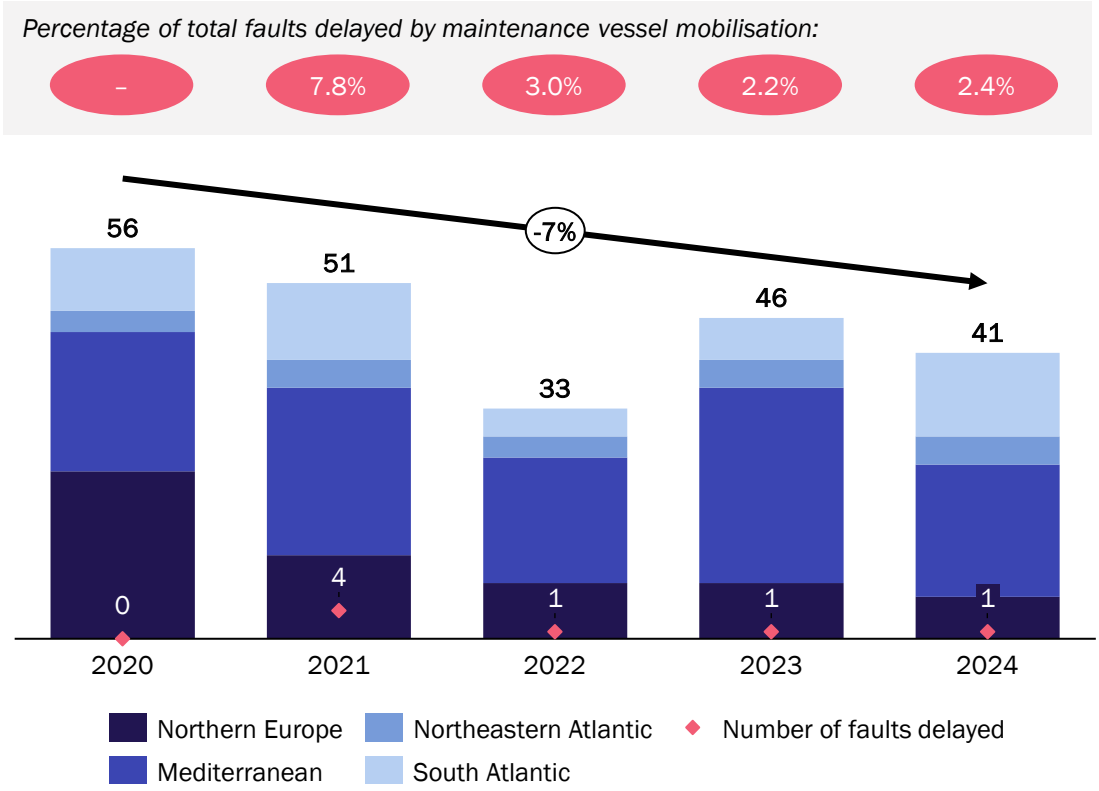
- ACMA
- APMA
- MECMA
- regional private agreements in the Baltic Sea.

Specifically for ACMA and APMA, which cover the entire Atlantic region, only submarine cable faults relevant to EU Member States have been considered in the analysis (i.e., faults within one of the regions defined in Section 3.1 of this report).

The total number of faults reported between 2020 and 2024 by European region is provided in Figure 4.26, below.

([222]) Europacable for Submarine Cable Infrastructure Expert Group (non-public).

Figure 4.26: Total number of submarine cable faults and faults delayed by maintenance vessel mobilisation, by region [Source: APMA, ACMA, MECMA, Baltic Offshore, 2025]



As shown in Figure 4.26 above, the total number of faults across all European regions has decreased at a Compound Annual Growth Rate (CAGR) of around 7% year-on-year, despite an increase in the number of submarine cables deployed in the region. Insights gathered from industry interviews, conducted by Analysys Mason and Axiom to inform and support the findings of this report, suggest that the decline in the number of faults is mainly attributed to:

- better education of the fishing community
- better submarine cable laying standards and route planning
- technological advancements in cable design.

Regarding Northern Europe, which includes the Baltic Sea basin, Figure 4.26 shows that the number of faults has decreased at a faster rate (at a CAGR of 29% year-on-year since 2020) than the average rate for all European regions. This is predominantly caused by the decommissioning of TAT-14 and SMW3 in 2020 and 2024, respectively. These submarine cables were laid in areas of intense fishing activity and were not adequately buried, resulting in frequent damage from trawling.

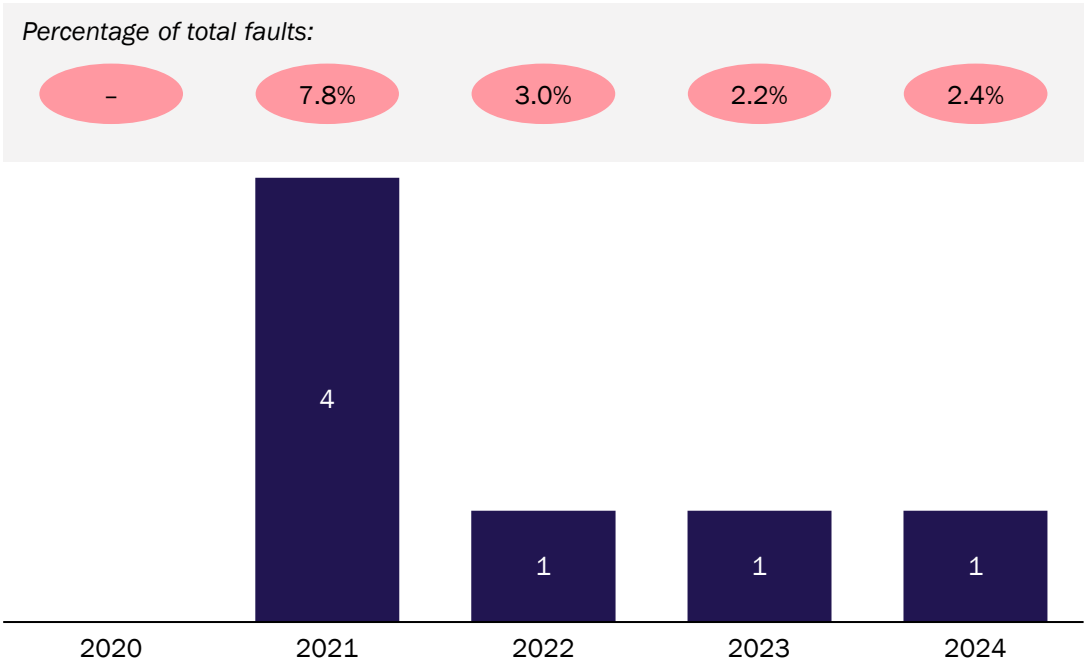
As mentioned in Section 3.3.2, although projections indicate that the number of submarine cable faults in Europe will increase somewhat from 41 faults in 2024 to 48 in 2025, ([161]) this would remain within the range of recent historical fault data reported by maintenance providers.

4.6.2. Analysis of vessel mobilisation time

In addition to tracking the overall number of faults, another useful indicator to determine whether the current maintenance fleet is sufficient to repair and maintain the existing submarine cables across the various European regions is the number of faults where cable owners had to wait for a repair vessel to be mobilised because it was already repairing another fault when the cable owner notified the maintenance provider.

Figure 4.27 shows the total number of faults where vessel mobilisation was delayed because the vessel was already deployed on another repair when the notification was received from the cable owner.

Figure 4.27: Number of faults delayed by maintenance vessel mobilisation [Source: APMA, ACMA, MECMA, Baltic Sea maintenance providers, 2025]



As shown in Figure 4.27 above, only one fault was reported per year in 2022, 2023 and 2024 (across all European regions) where maintenance vessel mobilisation was delayed because it was dealing with another repair. This means that cable owners were likely to face repair delays in 2–3% of cases reported during this period. Under a business-as-usual scenario, dimensioning a fleet to ensure that at least one maintenance vessel is always ready for mobilisation in the event of a fault would be very costly and not a commercially viable model, as cable owners might be reluctant to pay for the additional costs.

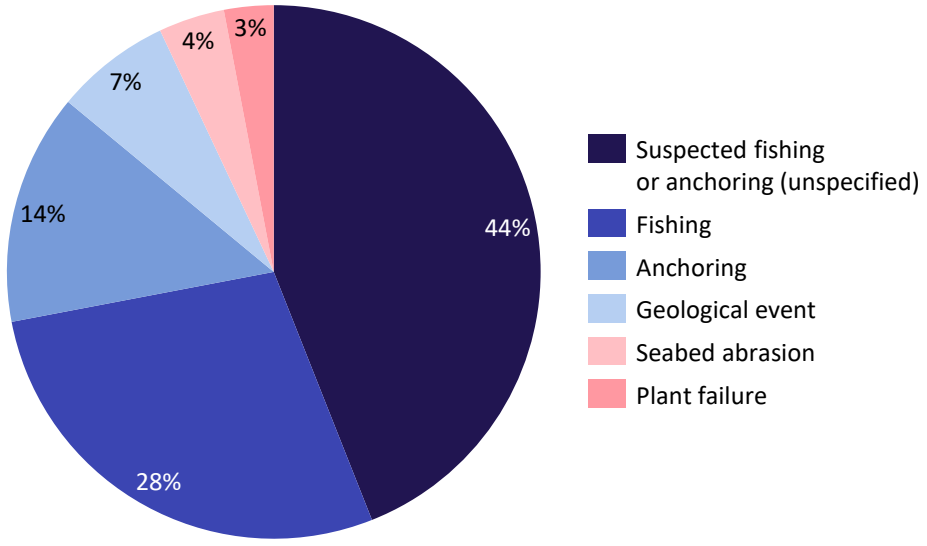
Finally, only one fault was reported in the Baltic Sea in 2022 where a maintenance vessel was not readily available to be deployed, causing repair delays.

4.6.3. Analysis of fault causes in Europe

Cable faults can be caused by a variety of reasons, as shown in Figure 4.28 below. Approximately 42% of submarine cable faults are proven to be caused by fishing and anchoring. An additional 44% of faults are suspected to be caused by such activities, raising the total to up to 86%. Determining whether a fault was caused intentionally or not can be very challenging, as recent incidents have demonstrated. ([223]) However, faults are generally presumed to be unintentional.

Figure 4.28 also shows that some cable faults are caused by natural phenomena such as bottom currents and undersea seismic activity, but this type of incidents only represent 11% of total faults. The remaining 3% of faults are related to plant failure.

Figure 4.28: Main causes of submarine cable faults [Source: International Cable Protection Committee, 2025]



4.6.4. Permits

As outlined in Section 4.4.5, a major factor influencing repair times is the time it takes to obtain the necessary permits to repair a submarine cable.

This process varies significantly across European regions. In the Baltic Sea Basin, for example, maintenance permits for submarine cables typically have a duration of 1 to 3 years, while in the Atlantic Ocean and the Mediterranean Sea, a separate permit needs to be issued for each fault event, which can delay repairs and become a bottleneck in the overall maintenance timeline. This issue is exacerbated by the fact that, in some Member States, an operational permit is also required to enter EEZ waters. Any delay in obtaining the required permit would lead to delays in vessel mobilisation to minimise additional costs for the cable owner. However, it should be noted that increasing the number of maintenance vessels would not improve vessel mobilisation times in these situations.

([223]) Reuters (2025), *Swedish probe finds no conclusive evidence of deliberate cable damage by Chinese ship*.

4.7. Land-based infrastructure

Although the primary focus here is on submarine cables, the significant role of land-based cables in the European internet backbone should not be underestimated. Some EU Member States in continental Europe mainly depend on these for cross-border connections, while others achieve high redundancy by combining land and sea routes.

Generally, island States and ORs/OCTs are more susceptible to submarine cable failures due to their limited access to land-based fibre-optic networks.

Many EU Member States are interconnected to either other EU Member States or non-EU Member States through these land-based cables, where they share a land border.

4.8. Alternative infrastructure

While submarine cables remain the backbone of global data transmission, satellite networks, particularly Low-Earth Orbit (LEO) constellations, are increasingly being explored as complementary or backup solutions, especially in areas where cable deployment is impractical.

It is worth noting that LEO satellites are primarily used to provide broadband access especially in remote and underserved regions where deploying fixed infrastructure is difficult or too costly, and are not designed to match and/or replace submarine cable infrastructure. As of January 2025, the Starlink LEO satellite constellation had a total capacity of approximately 450 Tbit/s in the downlink and 50 Tbit/s in the uplink. ([224]) This means that if symmetrical capacity is considered, a full satellite constellation could only deliver approximately 10% of the capacity provided by a single submarine cable (for example, the Anjana cable has a design capacity of 480 Tbit/s). This does not account for the fact that, at any point in time, two thirds of Starlink's total capacity is underutilised, as satellites are crossing oceans while circling around the globe, where subscriber density is very low (i.e., they can only serve subscribers in ships and planes during those periods).

Finally, it should be noted that the current cost per Mbit/s for satellite services such as Starlink is estimated to be around 3000 times higher than the cost per Mbit/s associated with submarine cables. ([224])

As a result, satellites could offer a back-up solution for high-priority, low-traffic applications, such as voice communications in remote or emergency scenarios, but they lack the capacity to carry all the traffic that is currently served by submarine cables.

4.9. Data centres, cloud regions and internet exchanges

Data centres and internet exchanges are essential for global connectivity, as they store, manage and process vast amounts of data. Submarine cables connect these data centres across different continents, enabling fast data transmission and global communication. Internet exchanges help to route this data efficiently by allowing various networks to connect and exchange traffic, which reduces latency and enhances the performance of internet services.

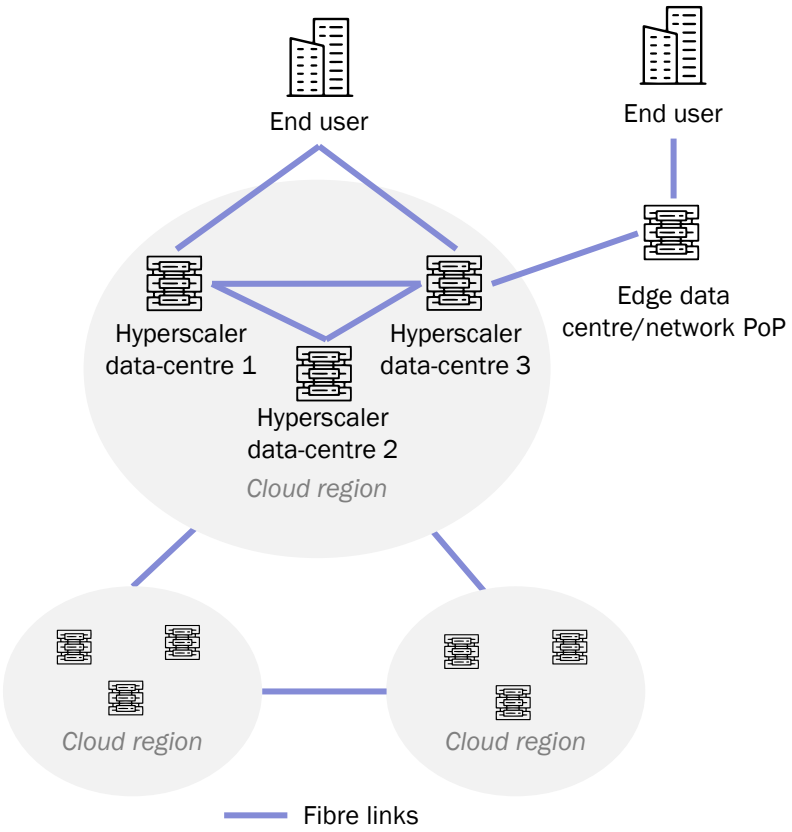
([224]) TeleGeography (2025), *Mythbusters V: Greaterst Hits*, SubOptic Ltd.

Cloud regions

Hyperscalers' infrastructure deployment typically begins with the deployment or leasing of data-centre space to create a network of points of presence (PoPs), to connect local clients to the hyperscaler's global network. Once there is sufficient local demand, hyperscalers generally deploy a local cloud region, which ensures increased performance for local customers and facilitates regulatory compliance (for example, complies with data residency and sovereignty requirements).

Cloud regions are typically composed of three or more large data centres, located in relative proximity and usually in a major city where there is strong local demand for hyperscale services: the duplication of data centres in a cloud region provides the necessary resilience for that region and the application load can be balanced across the region's data centres.

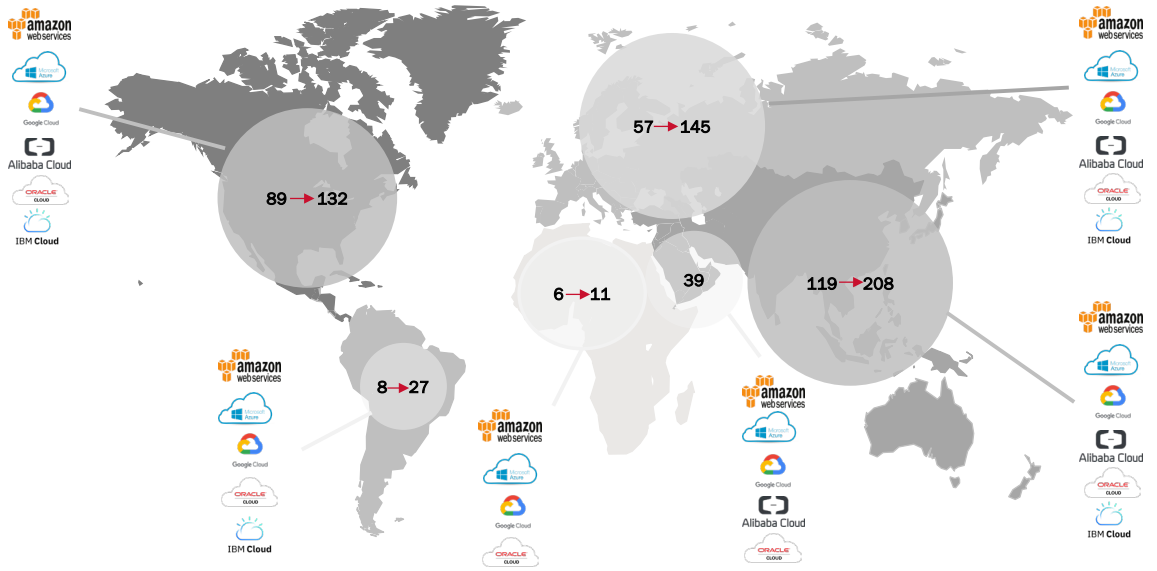
Figure 4.29: Illustration of hyperscaler infrastructure [Source: Analysys Mason, 2025]



Hyperscalers have more than doubled their number of cloud regions and availability zones over the last 5 years, to cope with the growing data-centre demand, reaching over 560 data centres by the fourth quarter of 2024 globally (see Figure 4.30). ([225]) There are also local cloud zones, which are typically individual data centres in a geographical region, without forming a cloud region.

([225]) Source: Analysys Mason.

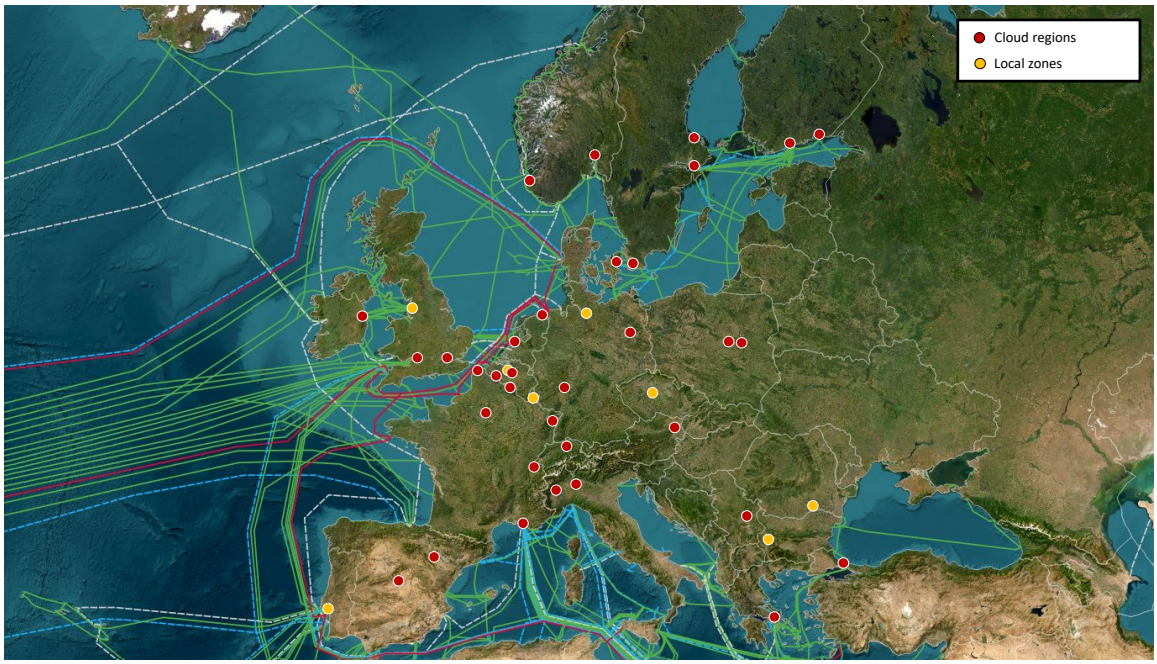
Figure 4.30: Geographical distribution of data centres for Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Alibaba Cloud, Oracle and IBM Cloud (2019 to Oct-2024) [Source: Cloud Service Provider (CSP) websites, Analysys Mason, 2024]



Hyperscalers have a strong presence in Western Europe, with several having cloud regions in multiple markets, and further expansions planned.

Figure 4.31 below shows how these data centres and cloud regions in Europe tend to be located on submarine cable hotspots, leading to a direct correlation between new data centres and demand for submarine cable capacity.

Figure 4.31: Map of European cloud infrastructure [Source: TeleGeography, Analysys Mason, 2025]



Internet exchanges

An Internet Exchange Point (IXP) is a physical place where different internet players such as ISPs and CDNs interconnect, in order to:

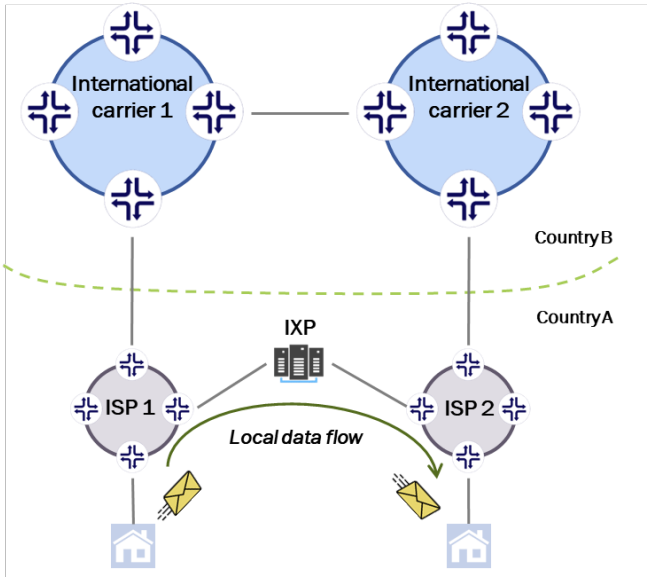
- improve the quality of their services
- reduce transit costs.

Under the NIS2 Directive, ([226]) the legal definition of an internet exchange point is "a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic".

Traffic going from one network to another would potentially rely on an intermediary network to carry the traffic from source to destination. This is how a large portion of international internet traffic flows, as it is not economically viable to maintain direct connections to each-and-every ISP in the world.

However, relying on a backbone ISP to carry local traffic can have an adverse effect on performance, sometimes due to the backbone carrier sending data to another network in a different country.

Figure 4.32: Schematic representation of an IXP [Source: Analysys Mason, 2025]



IXPs and submarine cables are crucial interconnected elements of the global internet infrastructure. Submarine cables allow for long-distance data transmission between continents, while IXPs enable efficient and cost-effective traffic exchange between networks on a more localised scale.

Once the data reaches a landing station from the submarine cable, it is then routed to IXPs, where it can be exchanged between different networks. Together, they ensure the smooth flow of data worldwide, supporting the internet's extensive and intricate ecosystem.

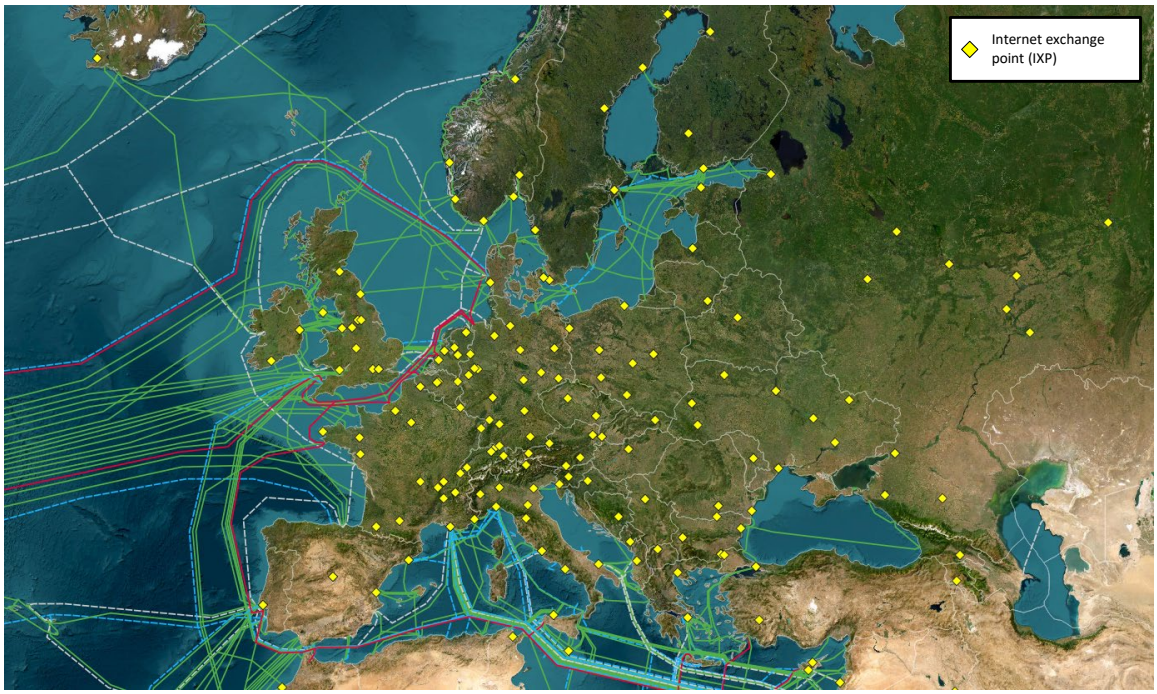
([226]) Article 6, point 18.

By connecting to IXPs, networks can exchange traffic locally rather than relying on long-distance routes. This reduces latency and improves the performance of internet services. Submarine cables play a crucial role in this process by providing high-capacity, low-latency connections between different regions.

Also, both IXPs and submarine cables contribute to the redundancy and reliability of the internet. If one path becomes unavailable, data can be rerouted through alternative paths, ensuring continuous connectivity. IXPs facilitate this by providing multiple interconnection points, while submarine cables offer diverse routes across oceans.

Finally, IXPs help to reduce the cost of data transmission by allowing networks to exchange traffic directly, avoiding the need for expensive transit through third-party networks. Submarine cables, on the other hand, provide a cost-effective means of transmitting large volumes of data across long distances.

Figure 4.33: Map of IXPs [Source: Analysys Mason, 2025]



Appendix A Abbreviations

Abbreviation	Definition
AAE	Asia Africa Europe
ACE	Africa Coast to Europe
ACGF	Arctic Coast Guard Forum
ACMA	Atlantic Cable Maintenance Agreement
ACPL	ASEAN Cableship Pte Ltd
AI	Artificial Intelligence
AIS	Automated Identification System
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APMA	Atlantic Private Maintenance Agreement
APMMSA	Asia Pacific Marine Maintenance Service Agreement
ASIC	Application-Specific Integrated Circuit
ASN	Alcatel Submarine Networks
AWS	Amazon Web Services
CDN	Content Delivery Network
CEF	Connecting Europe Facility
CER	Critical Entities Resilience
CISE	Common Information Sharing Environment
CMR	Critical Maritime Route
CSDP	Common Security and Defence Policy
CSP	Content Service Provider
DAS	Distributed Acoustic Sensing
DG CNECT	Directorate-General for Communications Networks, Content and Technology
DG MOVE	Directorate-General for Mobility and Transport
DNS	Domain Name System
DSP	Digital Signal Processor
ECGFF	European Coast Guard Functions Forum
EDA	European Defence Agency
EDFA	Erbium-Doped Fibre Amplifiers
EEA	European Environmental Agency
EEAS	European External Action Service
EEZ	Exclusive Economic Zone
EFCA	European Fishery Control Agency
EIB	European Investment Bank
EIG	Europe India Gateway
EMC	East to Med Corridor
EMEA	Europe, the Middle East and Africa
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUMSS	European Union Maritime Security Strategy

Abbreviation	Definition
EUR	Euro
EUROSUR	European Border Surveillance system
FAT	Factory Acceptance Test
GDP	Gross Domestic Product
HARMSPRO	Harbour and Maritime Surveillance and Protection
ICT	Information, Communications and Technology
IEX	India-Europe-Xpress
IMEWE	India-Middle East-Western Europe
EU-INTCEN	EU Intelligence and Situation Centre
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISPS	International Ship and Port Facility Security
IT	Information Technology
ITU	International Telecommunication Union
IXP	Internet Exchange Point
JBIC	Japan Bank for International Cooperation
JSMD	Joint System Maintenance Document
MARSUR	Maritime Surveillance project
MAS MCM	Maritime (semi-) Autonomous Systems for Mine Countermeasures
MEAE	Ministère de l'Europe et des Affaires Étrangères
MECMA	Mediterranean Cable Maintenance Agreement
MENA	Middle East and North Africa
MIC-RAN	Maritime Intelligence Community & Risk Analysis Network
MROSS	Multi Role Ocean Surveillance Ship
MS	Member State
MSSP	Managed Security Service Provider
MTBF	Mean Time between Failures
MUSAS	Maritime Unmanned Anti-Submarine System
NACGF	North Atlantic Coast Guard Forum
NATO	North Atlantic Treaty Organization
NAZ	North American Zone Cable Maintenance Agreement
NDICI	Neighbourhood, Development and International Cooperation Instrument
NEC	Nippon Electric Company
NEL	NTT Electronics
NIS	Network and Information Security
NOC	Network Operations Centre
NSW	Norddeutsche Seekabelwerke
NTT	Nippon Telegraph and Telephone
OADM	Optical Add-Drop Multiplexer

Abbreviation	Definition
OFS	Optical Fiber Solutions
OSS	Operational Support System
OTDR	Optical Time Domain Reflectometer
PA	Provisional Acceptance
PEACE	Pakistan and East Africa Connecting Europe
PESCO	Permanent Structured Cooperation
PFE	Power Feed Equipment
PLIB	Post Lay Inspection and Burial
RAN	Radio Access Network
RFS	Ready for Service
ROADM	Reconfigurable Optical Add-Drop Multiplexer
ROV	Remotely Operated Vehicle
SDM	Space Division Multiplexing
SEAIOCMA	South East Asia and Indian Oceans Cable Maintenance Agreement
SLTE	Submarine Line Terminating Equipment
SMF	Single-Mode Fibre
SPMA	South Pacific Maintenance Agreement
STC	Standard Telephones and Cables
TLD	Top-Level Domain
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UNODC	UN Office on Drugs and Crime
UPS	Uninterruptible Power Supply
US	United States of America
WACS	West Africa Cable System
SAT-3/WASC	South Atlantic 3/West Africa Submarine Cable
WDM	Wavelength Division Multiplexing

Appendix B Submarine cable installation fleet

Figure B.1: Global cable laying vessel fleet [Source: Analysys Mason, Axiom, ICPC 2025]

Owner	Vessel name	Country of registration	Baseport	Other capabilities	Cable capacity (tonnes)	Built year/refit	Age
ASN	Ile de Batz	France	France	Plough/ROV	6000	2001	24
	Ile de Bréhat	France	France	Plough (ROV capability)	6000	2002	23
	Ile de Sein	France	France	Plough (ROV capability)	6000	2001	24
	Ile d'Yeu	France	France	N/A	9600	2000	25
Elettra	Teliri	Italy	Italy	Plough/ROV	2500	1996	29
Orange Marine	René Descartes	France	France	Plough/ROV	5800	2002	23
E-Marine	Niwa	UAE	UAE	ROV and sea plough	6098	1991	34
Fiberhome	Feng Hua 21	China	China	N/A	Unknown	2021	4
Global Marine	CS Recorder	UK	UK	Plough/ROV	5200	2000	25
	Normand Clipper	Norway	Norway	Plough/ROV	5000	2001	24
Kokusai Cable Ship (KCS)	KDDI Cable Infinity	Japan	Japan	Plough	5000	2019	6
NTT	Subaru	Japan	Japan	Plough and ROV	4000	1998	27
OMS	Ile de Re	Indonesia	Indonesia	Plough/ROV	5040	1982	43
S. B. Submarine Systems	CS Bold Maverick	Panama	China	Maintenance, plough	5700	2001	24
	CS Fu Hai	Panama	China	Maintenance, ROV, HP-plough	5700	2000	25
	Fu Tai	Panama	China	Maintenance, ROV, HP-plough	3000	2007/2021	18
Subcom	Decisive	Marshall Islands	US	ROV, plough	5466	2003	22

Owner	Vessel name	Country of registration	Baseport	Other capabilities	Cable capacity (tonnes)	Built year/refit	Age
	Dependable	Marshall Islands	US	ROV, plough	5466	2002	23
	Durable	Marshall Islands	US	ROV, plough	5466	2002	23
	Endeavour	Marshall Islands	US	ROV, plough	5200	1999	26
	Global Sentinel	US	US	Plough/ROV	6098	1991	34
	Reliance	Marshall Islands	US	ROV, plough	5466	2001	24
	Resolute	Marshall Islands	US	ROV, plough	5466	2002	23
	Responder	Marshall Islands	US	ROV, plough	5466	2001	24

Appendix C Submarine cable maintenance fleet

Figure C.1: Global cable maintenance vessel fleet [Source: Analysys Mason, Axiom, ICPC, 2025]

Owner	Vessel name	Country of registration	Baseport	Other capabilities	Cable capacity (tonnes)([227])	Built year/refit	Age
Asean Cableship (ACPL)	CS Asean Explorer	Singapore	Sri Lanka	Plough/ROV	5760	2002	23
	CS Asean Restorer	Singapore	Singapore	Plough/ROV	2475	1994	31
ASN	Ile d'Aix	France	France	Cable installation and pre-lay grapnel runs	4000	1992	33
	Ile de Molène	France	Curaçao	Burial and pre-lay grapnel run	800	2006/2022	19
	Ile d'Ouessant	France	Cape Verde	ROV	225m^3	2011	14
Bina Nusantara Perkasa (BNP)	Nusantara Explorer	Indonesia	Indonesia	N/A	2970m^3	1996	29
Elettra	Antonio Meucci	Barbados	Italy	Plough/ROV	2600	1998	27
Orange Marine	Léon Thévenin	France	South Africa	ROV	1000	1983	42
	Pierre de Fermat	France	France	Plough/ROV	3400	2014	11
	Sophie Germain	France	France	ROV	1300	2023	2
E-Marine	CS Maram	UAE	UAE	ROV	2750	2016	9
	Etisalat	UAE	UAE	ROV	600	1990	35
	Umm Al Anber	UAE	UAE	ROV	4200	1972	53

([227]) Cable capacity for some vessels not available in tonnes.

Owner	Vessel name	Country of registration	Baseport	Other capabilities	Cable capacity (tonnes)([227])	Built year/refit	Age
Global Marine	C.S. Sovereign	UK	UK	Cable installation	6300	1991	34
	Cable Innovator	UK	US	Cable laying, plough/ROV	6999	1995	30
	Cable Retriever	Singapore	Philippines	ROV	7425	1997	28
	Wave Sentinel	UK	Curaçao	Cable installation, ROV	7800	1995	30
IT International Telecom	IT Intrepid	Barbados	Canada	Plough/ROV	1700	1989	36
Jala Nusantara Mardika	Pacific Guardian	Indonesia	Indonesia	N/A	Unknown	1984	41
Kokusai Cable Ship (KCS)	KDD Pacific Link	Japan	Japan	Plough	4500	1993	32
	KDDI Ocean Link	Japan	Japan	Plough/ROV	2300 m^3	1992	33
LS Marine Solution	Segero	Korea	Korea	Plough/ROV	3889	1999	26
Optic Marine	Cable Vigilance	France	France	Cable laying	Unknown	2006/2022	19
	Lodbrog	Malaysia	New Caledonia	ROV	5040	1985	40
	Peter Faber	France	Malaysia	ROV	575	1982	43
	Teneo	Indonesia	Indonesia	ROV	575	1992	33
Limin Marine & Offshore	Limin Venture	Indonesia	Indonesia	N/A	2300	1982	43
NTT	Kizuna	Japan	Japan	ROV	1652 m^3	2016	9
	Vega	Philippines	Philippines	Cable laying, ROV	169 m^3	1984	41

Appendix D Other submarine cable vessels

Figure D.1: Other submarine cable vessels [Source: Analysys Mason, Axiom, ICPL, 2025]

Owner	Vessel name	Country of registration	Baseport	Primary purpose	Other capabilities	Cable capacity (tonnes)([228])	Built year/refit	Age
Asean Cableship (ACPL)	CS Asean Protector	Singapore	Indonesia	Installation barge	Deep burial for shore ends	1000	2002	23
Baltic Offshore	Nordkable	Sweden	Sweden	Installation	Maintenance	120	1969	56
	Pleijel	Sweden	Sweden			1100	1989	36
E-Marine	CS Wasel	UAE	UAE	Installation support vessel – tugboat		Unknown	2014	11
Global Marine	CS Global Symphony	UK	UK	Installation for wind farms	Maintenance, plough/ROV	Unknown	2014	11
Lilaco Offshore	Telepaatti	Finland	Finland	Installation	Maintenance, cable recovery	250	1978	47
Mertech Marine	MV Aniek	Antigua and Barbuda	Antigua and Barbuda	Cable recovery		1327	1978/2009	47
	MV Layla	Antigua and Barbuda	Antigua and Barbuda	Cable recovery		1327	1975/2008	50
	MV Lida	Antigua and Barbuda	Antigua and Barbuda	Cable recovery		1230	1974/1999	51
OMS	Cable Empowered	Indonesia	Malaysia	Shallow water cable installation barge, also used in wind farms	Plough	450	2008	17

([228]) Cable capacity for some vessels not available in tonnes.

Owner	Vessel name	Country of registration	Baseport	Primary purpose	Other capabilities	Cable capacity (tonnes)([228])	Built year/refit	Age
	Cable Orchestra	Malaysia	Malaysia	Shallow water cable installation barge, also used in wind farms	Plough	706	Unknown	Unknown
Orange Marine	Raymond Croze	France	France	Maintenance (decommissioned)	N/A	1300	1983	42
Pirelli	Giulio Verne	Italy	Italy	Installation for power cables	Maintenance, plough and ROV	8000	1983	42
Seaway Offshore Cables	Seaway Aimery	Isle of Man	The Netherlands	Installation for power cables and wind farms	Maintenance, ROV	4250	2016	9
	Seaway Phoenix	Isle of Man	The Netherlands	Installation for power cables and wind farms	Maintenance, ROV	4000	2003	22
Subsea Environmental Services	MV Maasvliet	The Netherlands	The Netherlands	Cable recovery	N/A	2900 m^3	2025	<1
	MV Rebecca	The Netherlands	The Netherlands	Cable recovery	N/A	2900 m^3	2008	17