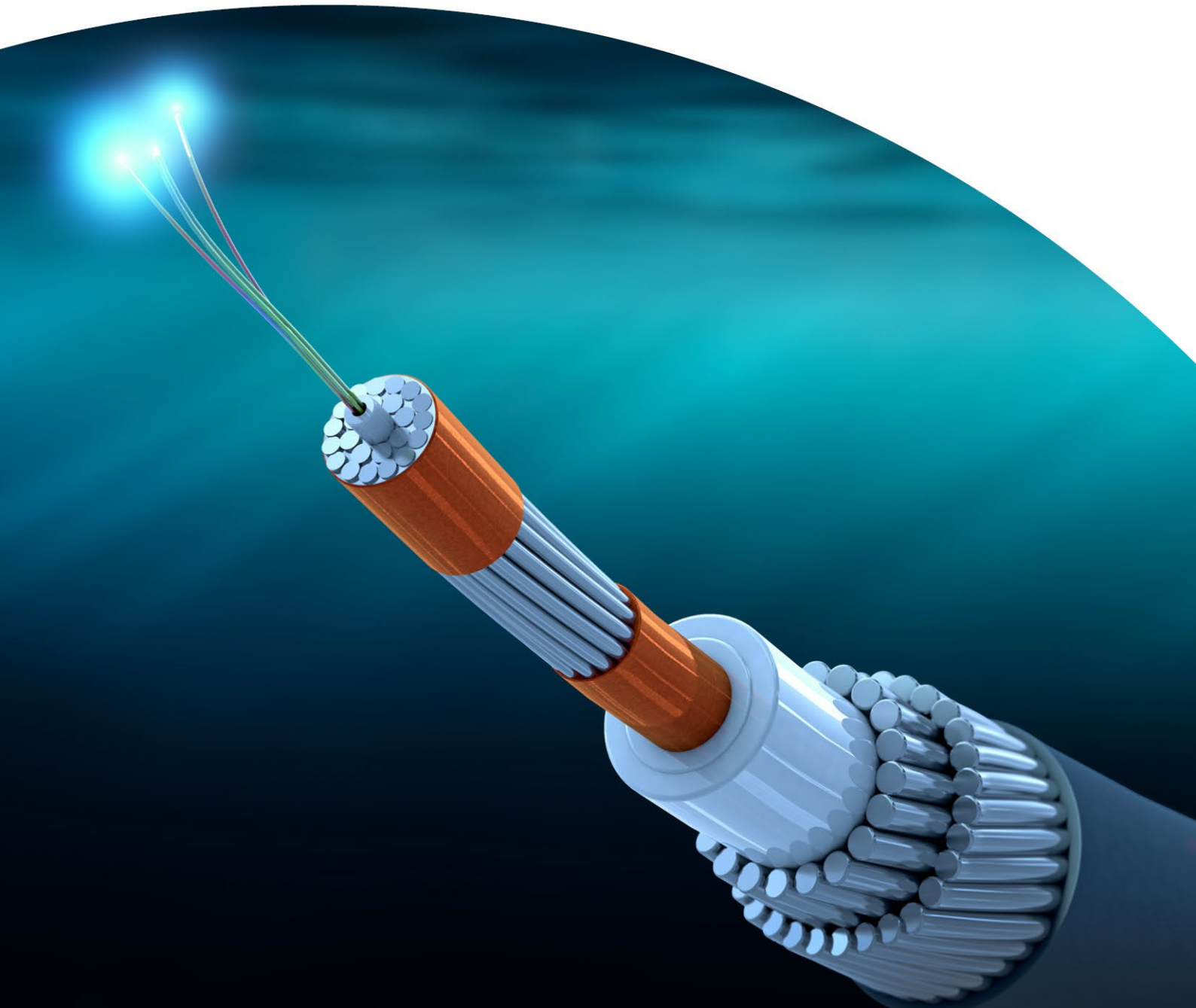
Report by the Expert Group under Recommendation 2024/779
on Secure and Resilient Submarine Cable Infrastructures

Security and Resilience of EU Submarine Cable Infrastructures

Mapping, Risk Assessments, Stress Tests

Main report

October 2025



Date:	6 October 2025
Version:	6
Authors:	Submarine Cable Infrastructures informal Expert Group supported by Analysys Mason & Axiom under service contract EC-CNECT/2024/OP/0070
Revised by:	DG CNECT E.1
Approved by:	DG CNECT

Table of Contents

1. INTRODUCTION

Amid rising geopolitical tensions, submarine cables connecting Europe have suffered multiple incidents in recent years (although the nature of these events, whether accidental or intentional, is not always easy to determine). These incidents have raised awareness across Europe and beyond regarding the criticality and vulnerability of submarine cables carrying data, gas or electricity.

To address these concerns, the European Commission ('the Commission') and the High Representative of the Union for Foreign Affairs and Security Policy ('the High Representative') adopted the EU Action Plan on Cable Security ([1]) on 21 February 2025 (the 'Cable Action Plan'). This initiative outlines a series of coordinated actions to counter threats and enhance the resilience of telecoms and power submarine cable infrastructures, across all stages of the resilience cycle: prevention, detection, response and recovery, and deterrence.

The Cable Action Plan builds on previous initiatives, particularly the Commission Recommendation (EU) 2024/779 ([2]) on Secure and Resilient Submarine Cable Infrastructures, which focuses specifically on data cables. This Recommendation and the Cable Action Plan notably follow the 2022 Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (the 'Critical Infrastructure Council Recommendation'), ([3]) as well as the Directive on a high common level of cybersecurity across the Union (the 'NIS 2 Directive') ([4]) and the Directive on the resilience of critical entities (the 'CER Directive'). ([5])

To support the implementation of Recommendation (EU) 2024/779, the Commission set up the Submarine Cable Infrastructures Expert Group ('the Expert Group'), comprising representatives from Member States' authorities and the EU Agency for Cybersecurity (ENISA), to offer guidance particularly on the following matters that fall within the scope of the Recommendation:

- mapping the existing and planned submarine cable infrastructures at EU level, based on national mapping exercises
- conducting a consolidated Union-wide assessment of risks, including threats, vulnerabilities and dependencies of submarine cable infrastructures
- putting forward a Cable Security Toolbox of mitigating measures
- proposing a draft list of strategic Cable Projects of European Interest (CPEIs) that meet the criteria listed in Recommendation (EU) 2024/779
- advising on maintenance and repair capacity for submarine cables.

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

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

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

([4]) European Commission (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) (Text with EEA relevance) Text with EEA relevance*.

([5]) European Commission (2022), *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)*.

The Expert Group has adopted this report on the basis of a study contracted by the Commission ([6]) and informed by discussions and written exchanges between Member States and the Commission throughout 2024 and 2025.

The main body of the report provides key insights regarding the context and mapping of data cable infrastructures, the risk assessment approach and the stress test methodology. Complementary factual information is provided in the Annex. The Cable Security Toolbox and a priority list of CPEIs will be covered in a subsequent report by the Expert Group.

([6]) Study conducted by Analysys Mason and Axiom under service contract EC-CNECT/2024/OP/0070.

2. POLICY AND MARKET OVERVIEW OF SUBMARINE CABLE INFRASTRUCTURES

Relevant legislation and policies (at international, EU and national levels) span a range of areas, some of which are specifically focused on submarine cable infrastructures (for example, Recommendation (EU) 2024/779 and the Cable Action Plan), while others address cables as part of a broader scope of issues. Maritime security, physical security and cybersecurity are the principal policy domains that are directly relevant to the security and resilience of submarine cable infrastructures. However, several other aspects must be considered, such as maritime governance (established notably under the United Nations Convention on the Law of the Sea (UNCLOS)), competitiveness, economic security, technological sovereignty, internal security, defence and external action, including collaboration with the North Atlantic Treaty Organization (NATO) and other multilateral organisations.

The Annex to this report provides an overview of policy, legal and administrative aspects that are relevant to submarine cable infrastructures, both at the EU level and at the national level. It draws on feedback from EU Member States, gathered via a survey conducted by the Expert Group in 2024, as well as the aforementioned study contracted by the Commission.

The Annex also examines the submarine data cable market, value chain and ecosystem, and identifies several key findings that are relevant to EU policy development on the security and resilience of these infrastructures (and potentially other submarine infrastructures), notably:

- Approximately 97–98% of the global Internet traffic transits through submarine cables. Despite its significant terrestrial network infrastructure, the EU is not less reliant on submarine cables than other regions in the world. It is therefore **critical for the EU's economic security** to have resilient submarine cable infrastructures and reduce its dependency on non-EU entities, just as it is for the EU's competitors.

- The share of submarine cable capacity held by traditional telecoms operators in the EU has decreased rapidly in the last 10 years, whereas **US hyperscalers are steadily expanding their footprint**. Hyperscalers already own 90% of the total capacity on the cable route connecting the US and Europe, and are increasing their share on the Europe-to-Africa and Europe-to-Asia routes.

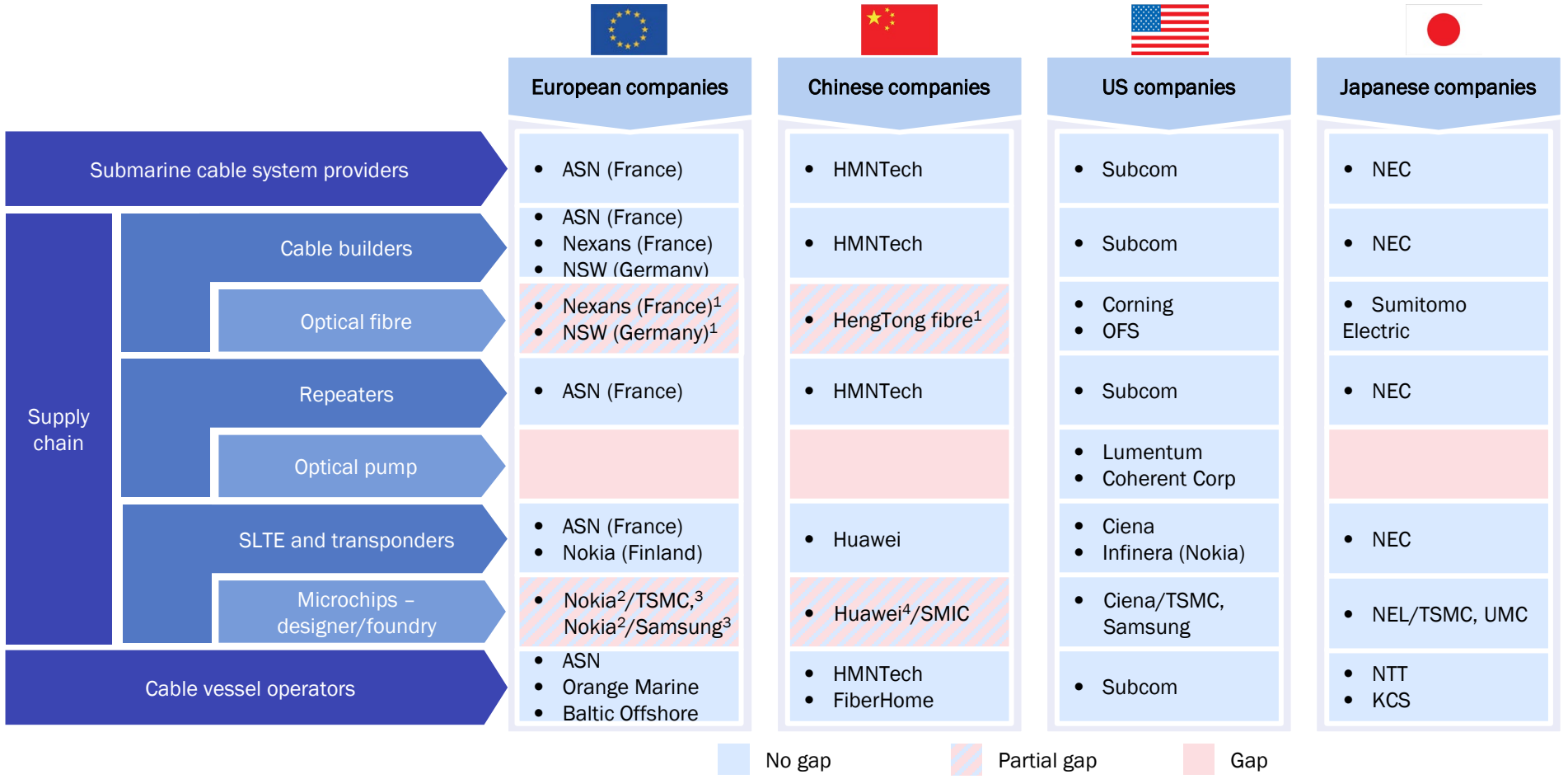
- **The lack of European investment in cross-continental submarine cables** implies that EU Member States rely significantly on submarine cables deployed by non-EU players for their capacity requirements on some routes.

- **Investment** by traditional telecoms operators **in regional cable systems has declined**, constrained by financial pressures and modest commercial prospects, largely due to reduced traffic on these secondary routes and rising competition from other players.

- There are also **pressures on cable repair capacity,** due to the ageing maintenance fleet and a substantial increase in the total length of cable installed by hyperscalers, which absorbs a significant portion of repair resources. Moreover, some repair vessels have been repurposed into installation vessels to meet the growing demand for submarine cable deployments (mostly from hyperscalers), while some hyperscalers may consider developing their own cable repair capacity.

- Finally, the EU has strong capabilities in cable installation and maintenance (Alcatel Submarine Networks (ASN), headquartered in France, is one of the three main global suppliers of submarine cables). However, the EU also has a **critical dependency on non-EU entities in the cable supply chain** (for example, optical fibre for long-haul submarine cables is exclusively manufactured by US and Japanese companies; optical pumps in repeaters are only manufactured by US companies; production and supply of microchips for transponders are largely controlled by Taiwanese and Korean providers; see Figure 2.1 below).

Figure 2.1: Key players and EU supplier dependencies in the submarine cable ecosystem ([7]) [Source: Analysys Mason/Axiom, 2024]



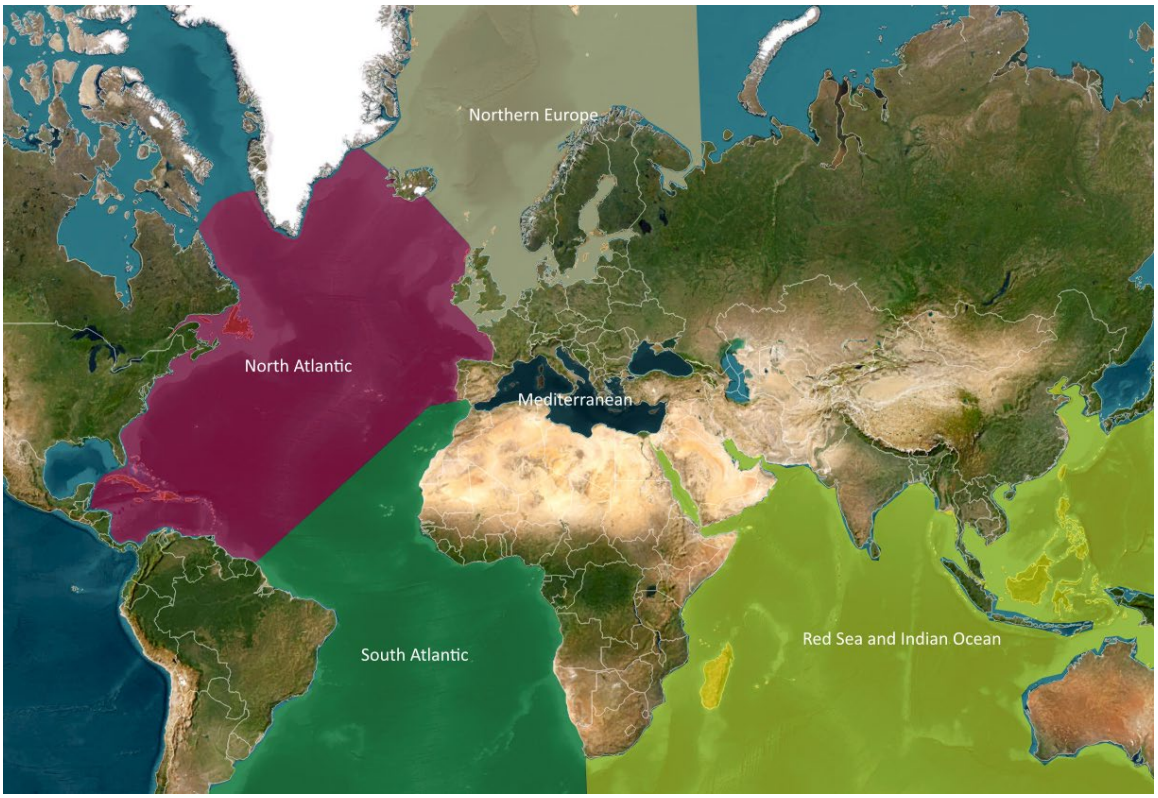
([7]) (1) Only for small unrepeated submarine cable systems; (2) Lack of state-of-the-art European foundry, although TSMC is building a new plant in Germany to mitigate Chinese take-over threat; (3) TSMC (Taiwan, under US influence) and Samsung (South Korea); (4) The US is preventing TSMC from providing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

3. MAPPING OF CABLE INFRASTRUCTURES 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 examines both types of infrastructure and associated capacity across various European regions, and analyses submarine cable faults in Europe to identify potential gaps in existing maintenance capabilities.

The region definitions used in this report are illustrated in Figure 3.1 (see details in Section 3.2 of the Annex).

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



3.1. Capacity analysis

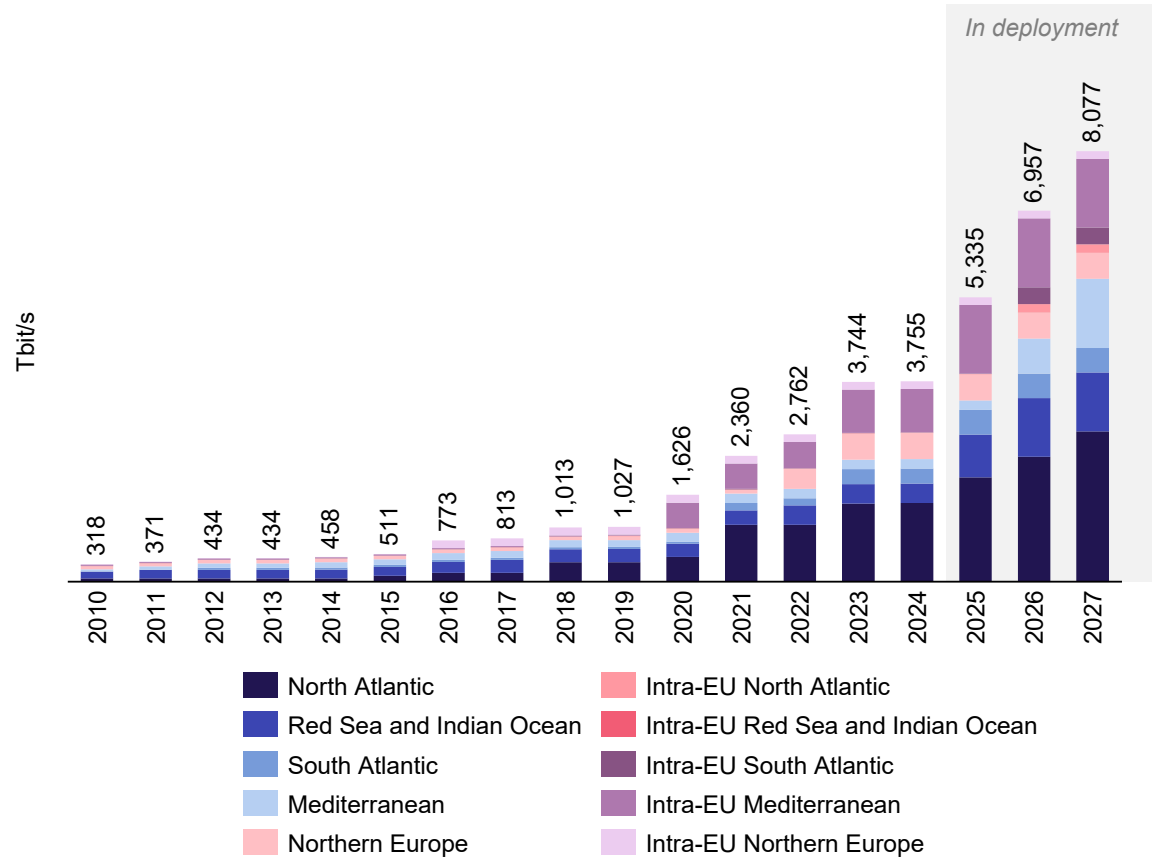
The expansion of submarine cable capacity over the past 10 years has primarily been driven by the increasing demand for international bandwidth from the four-largest hyperscalers (Google, Meta, Microsoft and Amazon). The requirement for these hyperscalers to interconnect their cloud regions in different continents has been shaping the industry in terms of capacity. On the transatlantic route, capacity ownership is fully dominated by hyperscalers due to their need to interconnect the US and European cloud regions. European investments in transatlantic submarine cable projects remain limited in comparison to the US, due to the fact that Europe does not have its 'own hyperscaler' and that traditional telecoms operators and carriers do not have the sufficient volume of traffic to justify such investment.

In the Red Sea and Indian Ocean region, hyperscalers' own capacity is currently limited due to the underdeveloped cloud infrastructure in the Middle East and Asia. However, with three large-capacity cables under deployment, ([8]) they will soon gain access to significant capacity through their respective consortia.

This means that, if the current trend continues, EU Member States will become increasingly reliant on external players for their own connectivity needs to North America and potentially Asia and Africa, which raises concerns regarding the EU's technological sovereignty and economic security.

The 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 3.2. 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. ([9])

Figure 3.2: Submarine cable capacity landing in at least one EU Member State [Source: Analysys Mason, 2025]



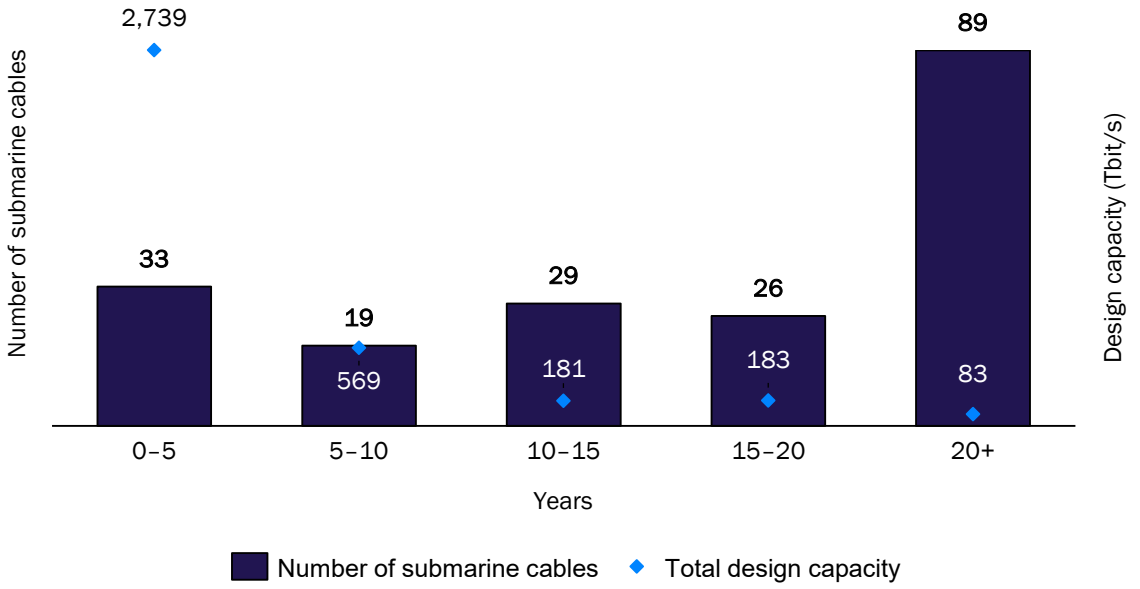
Submarine cables usually have a design life of 25 years, but it may potentially be extended if it proves economically viable. However, for most cables, their end-of-life is dictated by the deployment of the next generation of submarine cables, which eclipses the capacity of legacy cables and makes them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

([8]) Blue-Raman, India-Europe-Xpress (IEX) and SEA-ME-WE 6 (SMW6).

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

As shown in Figure 3.3, the 33 newest cables provide 74% of the total capacity currently provided by submarine cables landing in at least one EU Member State. In contrast, the 89 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 3.3: Number of submarine cables landing in the EU, total capacity and age in 2024 [Source: Analysys Mason, 2025] ([10])

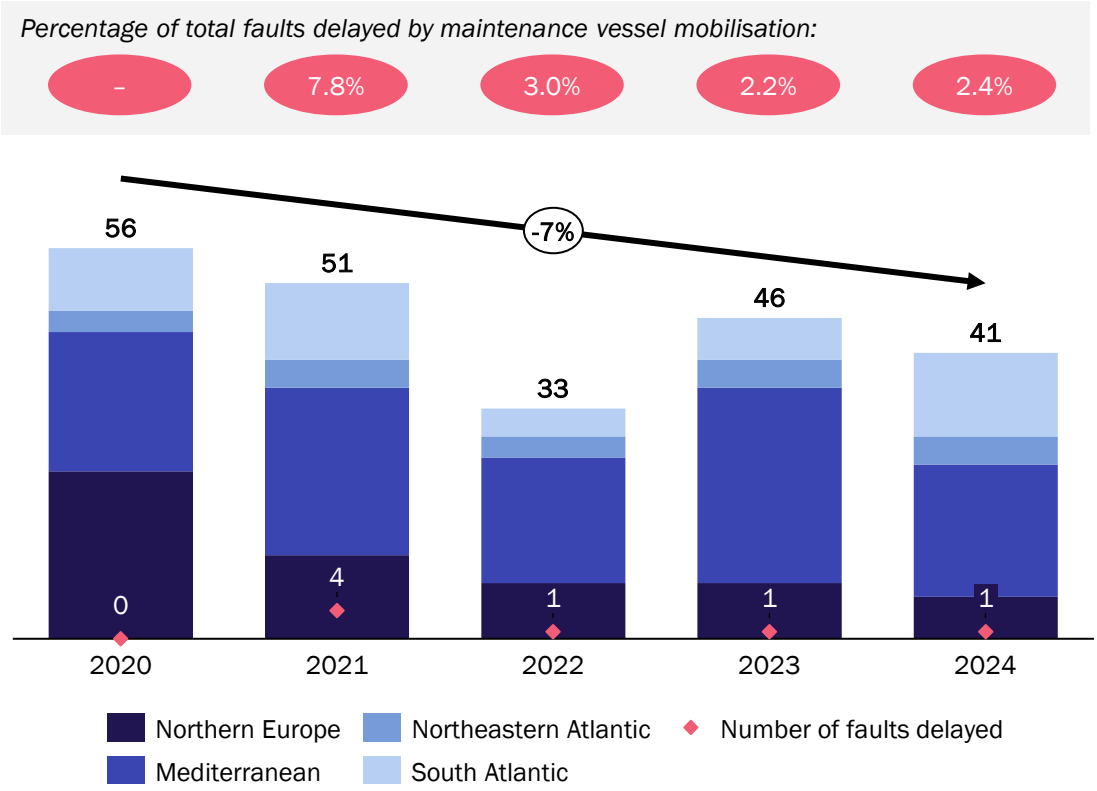


3.2. Fault analysis

The global number of submarine cable faults has remained relatively constant over the past 5 years, as documented by the International Cable Protection Committee (ICPC). However, in Europe, the number of reported incidents has reduced significantly, by 7% year-on-year, as shown in Figure 3.4, a trend which is accentuated in Northern Europe, where the volume of faults has decreased by 29% year-on-year since 2020. This decline in submarine cable faults is attributed to improved education within the fishing community, enhanced cable-laying standards implemented by companies, and improvements in cable design. It is also attributed to the decommissioning of the TAT-14 and SEA-ME-WE 3 (SMW3) submarine cables, which were located in shallow waters and not correctly buried.

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

Figure 3.4: Total number of submarine cable faults and faults delayed by maintenance vessel mobilisation, by region [Source: APMA, ACMA, MECMA, Baltic Offshore, 2025]



As illustrated in Figure 3.4 above, on average and across the entire European region between 2022 and 2024, there has been only one instance annually in which a repair vessel could not be mobilised within 24 hours due to being engaged in another repair, which represents between 2% and 3% of the total number of reported incidents (thus, 2021 can be considered an exception to this trend). Importantly, in the past 4 years, multipurpose vessel maintenance providers in the Baltic Sea have consistently mobilised to repair unrepeated cables within 24 hours, with no instances of delays due to insufficient maintenance vessels.

The declining number of faults, together with the ability to mobilise a vessel within 24 hours (excluding permitting delays), suggests that the current vessel fleet is adequate for maintaining repair times under business-as-usual conditions.

Although the fleet of maintenance vessels seems adequate under the current conditions, a reduction in the number of maintenance vessels could significantly affect the repair time. Causes for a reduction in the number of vessels may include:

- a lack of replacement of end-of-life vessels, or
- a new company acquiring an existing maintenance company and relocating the fleet in another region of the world, or
- a hyperscaler acquiring an existing maintenance company and exclusively using the fleet for its own purposes, or
- damage to one or several vessels.

TeleGeography forecasts that the volume of faults in Europe is expected to rise to 52 faults in 2035, representing a 27% increase compared to 2024. ([11]) Therefore, any reduction in the number of vessels may mean that the maintenance fleet would not be sufficient to repair all faults in a timely manner. Therefore, preserving the existing maintenance capability should be a focus for the EU.

Based on industry data collected for this report, ([12]) it is understood that the process to obtain operational permits differs significantly across European regions. For example, in the Atlantic Ocean and Mediterranean Sea, it could take between a few days and 4 weeks to obtain an operational permit to access territorial waters. In contrast, the Baltic Sea benefits from operational permits which are valid for 1 to 3 years, eliminating the need to request individual permits for each repair and consequently reducing repair time. These differences exist within the EU, however, the overall situation remains comparatively better than in other world regions, such as parts of Asia, where permitting processes can be significantly more complex and time consuming. Simplifying the permitting process across all Member States (e.g., the permit conditions imposed by legislation) would therefore benefit the repair time. Also, it would be beneficial for the EU to negotiate with non-EU countries (for example, North African countries in the Mediterranean Sea Bassin) to simplify the permitting process in regions where EU and non-EU countries are closely interlinked. These negotiations and any potential agreements should be based on the provisions of UNCLOS.

3.3. Related EU data infrastructures

Main landing stations

Despite the EU's extensive network of over 300 submarine cable landing stations and ongoing efforts to diversify landing locations, there remains a significant dependency on a few critical points. Specifically, the Red Sea remains a bottleneck, as 90% of the traffic between Europe and Asia transits through this corridor.

Some key landing stations (for example, Marseille (France) and Sines (Portugal)) have already been designed to be geographically redundant, which is crucial for major landing locations to minimise the impact of any cable damage.

Europe's geographical layout increases its susceptibility to threats. Several submarine cables connect remote island territories and span waters between Member States, making them vulnerable to disruption. In addition, island Member States (Cyprus, Ireland and Malta) rely almost exclusively on submarine cables for Internet connectivity, which means that the geographical diversity of landing stations and the resilience of individual landing stations is even more critical than for other Member States.

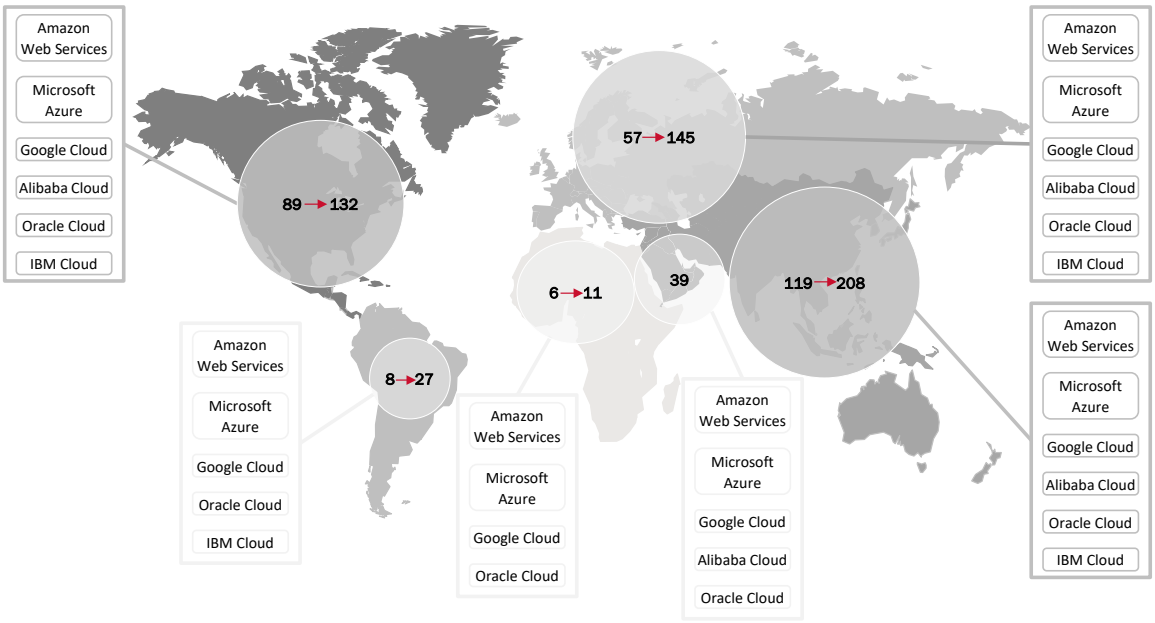
Data centres and cloud regions

The number of data centres and cloud regions in the EU is experiencing significant expansion, as shown in Figure 3.5, which is crucial for supporting the digital economy and ensuring data sovereignty. However, several gaps and challenges remain that need to be addressed to enhance the resilience and efficiency of these infrastructures.

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

([12]) Data collected is commercially sensitive and therefore cannot be explicitly mentioned in this report.

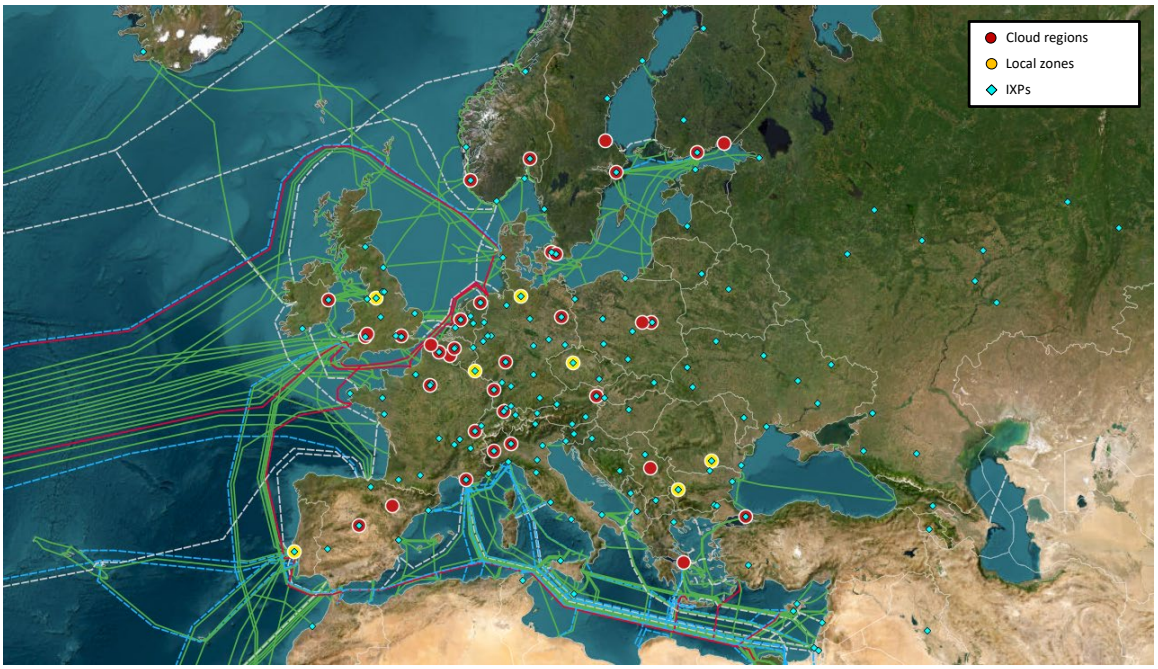
Figure 3.5: Geographical distribution of data centres for Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Alibaba Cloud, Oracle and IBM Cloud (2019 to Oct-2024) [Source: Cloud Service Provider (CSP) websites, Analysys Mason, 2024]



One of the primary challenges affecting submarine cable infrastructures is Europe's sovereignty over cloud solutions. Given the dominance of US hyperscalers, the EU needs to strike a balance between fostering its domestic cloud industry and ensuring collaboration with non-EU players to access the required essential technologies.

Furthermore, efficient and resilient connectivity between data centres and submarine cable landing stations is crucial for seamless data flows and to minimise latency. In this regard, land-based infrastructure must also be a key focus. The interplay between submarine cables, cloud infrastructure and Internet Exchange Points (IXPs) is demonstrated in Figure 3.6.

Figure 3.6: Map of European cables, cloud regions and IXPs [Source: TeleGeography, Analysys Mason, 2025]



As Mario Draghi stated in 2024, "it is too late for the EU to try and develop systematic challengers to the major US cloud providers". However, "the EU should ensure that it has a competitive domestic industry that can meet the demand for 'sovereign cloud' solutions". ([13])

Since the network of IXPs, data centres and cloud regions is directly connected to submarine cable infrastructures, improving the interconnection between these infrastructures is also essential for building a resilient digital economy and society in the EU more generally.

Alternative infrastructures

Low-Earth Orbit (LEO) satellites offer valuable connectivity in remote and undeserved areas. However, they are not designed to replace submarine cables. Their overall capacity and efficiency remains significantly lower than that of modern submarine cable systems. For example, the most advanced satellite constellations deliver only a fraction of the bandwidth provided by a single cable, and much of their capacity is underutilised while orbiting low-density regions. Consequently, satellites may serve as a useful backup for critical, low-bandwidth applications, such as emergency communications, but cannot replace the vast data volumes currently handled by submarine infrastructures.

([13]) Mario Draghi (2024), *The Future of European Competitiveness—A Competitiveness Strategy for Europe*, European Commission.

4. EU RISK ASSESSMENT

Recommendation (EU) 2024/779 proposes that the Expert Group assists the Commission in establishing the baseline for a consolidated Union-wide assessment of risks, including threats, vulnerabilities and dependencies. This is also a key action under the 2025 EU Action Plan on Cable Security. This section starts by providing an overview of relevant non-EU actors and then presents the approach for the EU risk assessment on the security and resilience on submarine cable infrastructures, as agreed by the Expert Group.

4.1. Non-EU actors relevant to resilience of EU cable infrastructures

The majority of incidents affecting submarine cables relate to unintentional activity by non-State actors as well as natural events, as detailed in the fault cause analysis in Section 4.6 of the Annex. These may involve fishing vessels damaging cables through bottom trawling; other commercial vessels causing damage to cables through anchoring, dredging and deep-sea mining; and cable faults caused by natural phenomena, such as bottom currents and undersea seismic activity (see Section 4.6 in the Annex for further details).

Nonetheless, several non-EU actors (both State and non-State actors) must be considered, either because their actions may pose direct security threats to submarine cable infrastructures with end points in the EU, or because of the EU's economic dependencies.

Regarding security threats, submarine cable infrastructures are obvious targets for grey zone warfare (i.e., actions that fall below the threshold of conventional warfare) and hybrid threats. Such threats involve harmful activities that are intentionally kept under the threshold of a full-scale armed conflict. The extensive nature of the maritime domain, where submarine cables are situated, combined with the involvement of numerous public and private entities, complicates the identification of the perpetrators. This complexity blurs the lines both between actions that are State-sponsored and those that are carried out by private actors, as well as between intentional and unintentional damage. Furthermore, the complexity and sheer scale of activities in this area make monitoring and surveillance challenging, despite significant technological advancements. The analysis below focuses on some key actors that are relevant for a comprehensive EU risk assessment.

With respect to economic dependencies, submarine cables are a critical infrastructure for the data economy as stressed earlier in this report. Therefore, the fact that certain cable routes are heavily linked to non-EU countries (e.g., as is the case for data traffic between Ireland and the rest of the EU, which largely transits through the UK) or controlled by non-EU companies (e.g., as is the case for US hyperscalers deploying cables between America and Europe) means the EU is dependent on non-EU actors for its economic stability.

Third countries and regions that may have an impact on the resilience of EU submarine cable infrastructures include in particular the following:

- **Rusia** – The ongoing Russian war of aggression against Ukraine and hybrid actions promoted by Russia against EU Member States has prompted European governments, defence forces and national security authorities to prioritise the potential threat from Russia to Europe's submarine cable infrastructures. Russia has conducted underwater military drills at depths exceeding 6000 metres, and its focus on transatlantic submarine cables has grown in recent years. ([14]) In 2023, NATO reported that Russia was 'actively mapping' the critical submarine infrastructure of

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

Ukraine's allies. ([15]) Additionally, NATO commanders publicly confirmed in April 2023 that they had noticed a rise in suspicious Russian activities around submarine cables in the Baltic Sea. ([16])

- **China** – In January 2024, the European Parliament passed a resolution on the security implications of Chinese influence on EU critical infrastructure, expressing "grave concern over the undersea data cable systems operated by Chinese company HMN Technologies". ([17]) The resolution underscored the importance of the cybersecurity vulnerabilities associated with cables installed and operated by Chinese companies (for example, the PEACE cable), including data collection, gathering of intelligence and underwater surveillance. Furthermore, in March 2025, the China Ship Scientific Research Centre (CSSRC) revealed that it had developed a remotely operated underwater vehicle capable of severing armoured submarine cables at depths up to 4000 metres. ([18])

- **Middle East** – Escalating instability across the Middle East in the context of Israel's military operations in the occupied Palestinian territories, and the resulting tensions between Israel and various regional governments and actors, poses a direct threat for data transmission via submarine cables connecting the EU and Asia. This includes the critical bottleneck of the Red Sea and the Bab El-Mandeb Strait. The hostilities against Western vessels by Yemenite Houthis in 2023 and 2024 provide a notable example of regional conflict affecting EU economic interests, as submarine cables get frequently cut in that region and the conflict makes it challenging to repair the affected cables. ([19])

- **Türkiye** – A stable and secure environment in the Mediterranean and the Black Sea is in the best interest of both the EU and Türkiye. Developing a cooperative and mutually beneficial relationship is key to fostering and preserving security, stability and connectivity in the wider region. At the same time, certain activities by Türkiye in the Mediterranean raise concerns, with implications for the EU and its Member States. A coordinated approach with Türkiye, an EU partner and a candidate country, is essential for enhancing stability, maritime safety, energy security and connectivity, in line with international law, including UNCLOS, and the principles of good neighbourly relations.

- **US** – The US plays a pivotal role in the submarine cable domain, not only through government initiatives, but also via its hyperscalers (Amazon, Google, Meta and Microsoft) which have significantly reshaped the submarine cable investment landscape, as documented earlier in this report. Additionally, there is a significant dependency on the US for the supply of crucial components of submarine cable systems, such as optical fibre ([20]) and optical pumps for repeaters. ([21]) It will be important to consider supply-related measures to mitigate the EU's economic dependency on the US.

([15]) Politico (2023), *NATO warns Russia could target undersea pipelines and cables*.

([16]) CNN Politics (2024), *US sees increasing risk of Russian 'sabotage' of key undersea cables by secretive military unit*.

([17]) European Parliament (2024), *Security and defence implications of China's influence on critical infrastructure in the European Union*.

([18]) Chen, S. (2025), *China unveils a powerful deep-sea cable cutter that could reset the world order*, South China Morning Post.

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

([20]) The US hosts two of the three optical fibre suppliers (i.e., Corning and OFS).

([21]) The two companies manufacturing global reliable optical pumps for submarine cable repeaters are based in the US.

- **UK** – The UK has historically been a crucial country for the landing of transatlantic submarine cables connecting the EU to North America and remains a strategic location after Brexit. Moreover, data traffic between Ireland and the rest of the EU largely transits through the UK. However, Member States such as Portugal, Spain, France, Ireland and Denmark are gaining strategic importance to mitigate Europe's reliance on the UK, and several new high-capacity transatlantic cables are now landing in these countries, such as MAREA (Spain) and Dunant (France). Nonetheless, submarine cable security is a mutual concern for both parties and collaboration is taking place between the UK and EU Member States. ([22]) For example, in April 2024, six North Sea countries (Belgium, Denmark, Germany, the Netherlands, Norway and the UK) published a joint declaration on cooperation regarding the protection of infrastructure in the North Sea. ([23]) This declaration highlighted the importance of improving information and knowledge sharing to better protect critical submarine infrastructures from foreign interference and disruption.

4.2. Consolidated threats, vulnerabilities and dependencies

The EU risk assessment presented in this report is based on a methodology agreed upon by the Expert Group following a Commission proposal. It draws on extensive desk research conducted by the Commission and was further refined through feedback from Expert Group members (including substantial contributions from Member State representatives and various Commission services).

After considering different **risk assessment methodologies**, the Expert Group eventually selected the 'EU methodology for Union-level cybersecurity risk assessments of critical supply chains' from the NIS Cooperation Group as the methodology framework to prepare the current risk assessment.

In a second step, information on potential **threats, vulnerabilities and dependencies** was collected through a dedicated questionnaire answered by Member States. Threats and vulnerabilities were grouped into categories related to intentional damage (both physical and cyber) and unintentional damage (human and natural). Dependencies were grouped into three categories: supply chain, geographical and technical/legal/administrative. The Expert Group agreed on the final list of consolidated treats, vulnerabilities and dependencies. The overall approach is summarised in Figure 4.1 below, while the complete list of threats, vulnerabilities and dependencies is captured in Figures 4.2, 4.3 and 4.4.

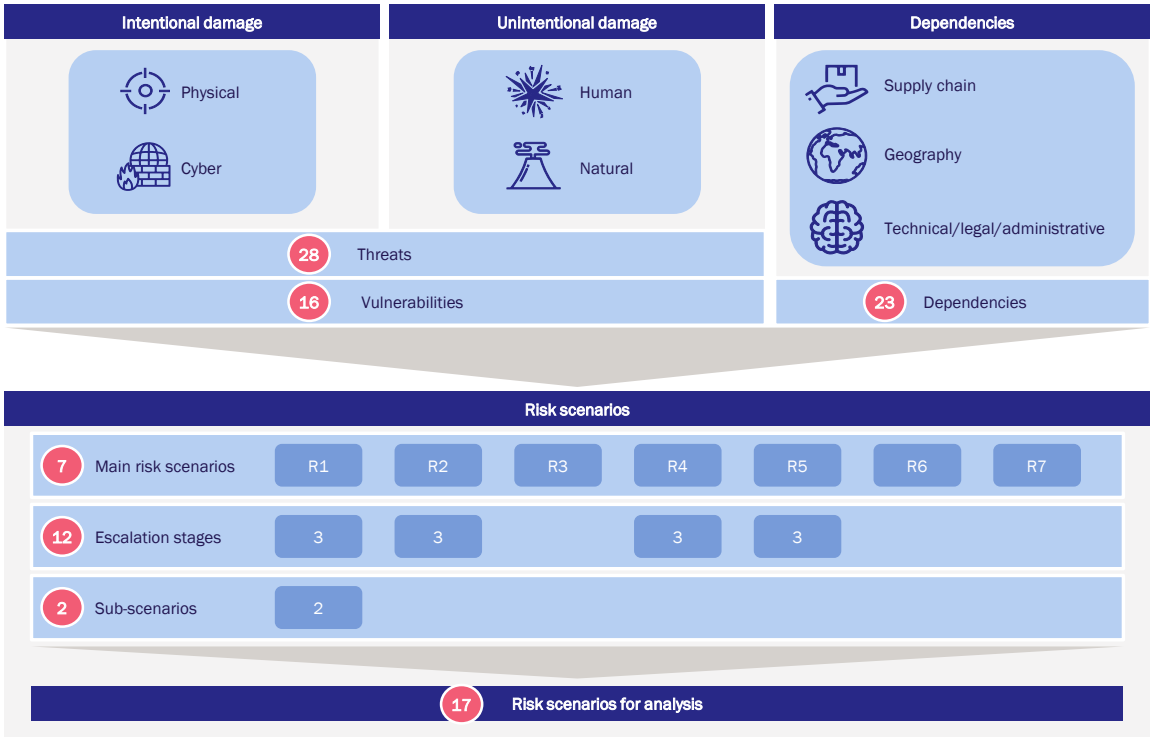
In a third step, **risk scenarios** were developed considering all identified threats, vulnerabilities and dependencies. For each risk scenario, estimations of impact and likelihood assessments were conducted, based on the definitions provided by the NIS Cooperation Group's methodology. ([24]) Moreover, in order to account for increasing levels of impact, **escalation stages** were defined for some scenarios, considering the risk posed to the EU as a whole (as opposed to the risk posed to individual Member States). Also, two sub-scenarios were developed for one scenario to consider the particular circumstances of islands and regions. To conclude, the Expert Group reviewed all this information and agreed to a final list of seven risk scenarios, which are detailed in the next section of this report.

([22]) Chapman, R. (2025), *The security of the UK's undersea critical national infrastructure*.

([23]) Norwegian Government (2024), *Six North Sea countries join forces to secure critical infrastructure*.

([24]) The Expert Group decided not to make this information public.

Figure 4.1: Risk assessment methodology [Source: Analysys Mason, 2025]



Based on the methodology described in Section 4.2, Figure 4.2, Figure 4.3 and Figure 4.4 below, respectively, provide a consolidated view of threats, vulnerabilities and dependencies across all Member States.

*Figure 4.2: Consolidated view of threats and vulnerabilities related to **intentional** submarine cable damage [Source: Analysys Mason, 2025]*

	Intentional damage	
	Physical	Cyber
Threats	• **T1.** Cable cuts in territorial waters • **T2.** Cable cuts in Exclusive Economic Zones (EEZs) • **T3.** Cable cuts in high seas • **T4.** Cable cuts in backhaul • **T5.** Damage/destruction of beach manhole • **T6.** Physical security breach at cable landing stations • **T7.** Damage/destruction of cable landing stations • **T8.** Power outage due to damage to grid/transformer • **T9.** Blockage of access to depot • **T10.** Damage to/destruction of depot • **T11.** Blockage of access to vessels • **T12.** Damage to/destruction of maintenance vessels • **T13.** Physical attack on the supply chain causing disruption	• **T14.** Network intrusion/intrusion into the operating system • **T15.** Insider threat • **T16.** Cybersecurity attack on a Managed (Security) Service Provider (M(S)SP) or other third-party service provider • **T17.** Cybersecurity attack on the supply chain causing disruption
Vulnerabilities	• **V1.** Insufficient physical security at beach manhole • **V2.** Insufficient physical security at cable landing station/Network Operation Centre (NOC) • **V3.** Insufficient physical security at depots • **V4.** Lack of depot backup location • **V5.** Exact position of cable, depots and cable landing station available in the public domain (eases targeting infrastructure by a third party) • **V6.** Lack of backup power supply at cable landing station	• **V7.** Insufficient cybersecurity in network management • **V8.** Insufficient cybersecurity of network equipment • **V9.** Insufficient cybersecurity of end-user devices

*Figure 4.3: Consolidated view of threats and vulnerabilities related to **unintentional** submarine cable damage [Source: Analysys Mason, 2025]*

	Unintentional damage	
	Human	Natural
Threats	• **T18.** Fishing (cable cut) • **T19.** Anchors (cable cut) • **T20.** Civil works and dredging (cable cut) • **T21.** Deep sea mining (cable cut) • **T22.** Misconfiguration of network	• **T23.** Undersea seismic activity • **T24.** Undersea volcanos • **T25.** Slumping • **T26.** Beach erosion • **T27.** Bottom current • **T28.** Adverse weather events
Vulnerabilities	• **V10.** Lack of education on submarine cables for the fishing industry • **V11.** Lack of protection area around the submarine cable route in territorial waters	• **V12.** Cables located in geographically unstable areas
	• **V13.** Unreliable network equipment • **V14.** Exposed cable at fishing/anchoring depth • **V15.** Lack of cable armouring at fishing/anchoring depth • **V16.** Lack of surveillance/advanced monitoring systems	

*Figure 4.4: Consolidated view of **dependencies** [Source: Analysys Mason, 2025]*

Dependencies		
 Supply chain	 Geography	 Technical/ legal/administrative
• **D1.** Supplier dependency (in particular non-EU) • **D2.** Lack of components due to nation state influence/control of supplier • **D3.** Lack of components in the market due to high demand or insufficient supply • **D4.** Lack of standardisation in submarine system components • **D5.** Shifting market demand from telecoms towards hyperscaler (data centres/AI) business model • **D6.** Lack of maintenance capability in the EU • **D7.** Lack of EU shipyard capacity for building new vessels • **D8.** Dependency of power supply	• **D9.** US dependency • **D10.** UK dependency • **D11.** Chinese dependency • **D12.** Russian dependency • **D13.** Cables located in geopolitically unstable areas • **D14.** Lack of route diversity • **D15.** Chokepoints	• **D16.** Dependency on technical expertise • **D17.** Long process to obtain repair permit • **D18**. Lack of jurisdiction for incidents in EEZs and high seas • **D19.** Lack of plan to respond to emergency situations • **D20.** Lack of centralised reporting of physical and/or cyber incidents • **D21.** Lack of co-ordination entity in each Member State or between countries to respond to a submarine cable incident or emergency situation • **D22.** Lack of information sharing between public entities from different Member States • **D23.** Lack of public–private co-ordination

4.3. Definition of risk scenarios

Based on the consolidated threats, vulnerabilities and dependencies outlined in the previous section of this report, seven risk scenarios were defined, with their respective impact (I) and likelihood (L), (although the Expert Group decided not to make the information on impact and likelihood of the risk scenarios public). Some of the defined scenarios are already referenced in the Nevers Report at a high level. ([25]) However, these have been adjusted, where appropriate, to better align with the specific context of submarine cable infrastructures. Also, three stages of escalation (E) have been developed for four of the seven scenarios identified below, notably to reflect the higher impact of versions of a scenario as building block injects to conduct stress tests (see subsequent section). In addition, for the cable cut scenario (R1), two sub-scenarios are developed to reflect situations particularly relevant for certain Member States (i.e., cutting off an entire island or region).

Using the methodology explained in Section 4.2, the Expert Group has defined seven risk scenarios as listed below. These reflect an EU-wide perspective and may be adapted by Member States to include elements based on their national context.

R1. Co-ordinated physical sabotage or attack on a submarine cable (R6 in the Nevers Report)

Definition

A hostile actor launches a coordinated physical sabotage or attack on multiple redundant but geographically close submarine cables. The incident may be caused through the use of either anchor/grapnel, or a remotely operated vehicle to sever the cables, or through the placement of mines which could be detonated remotely. The intent of the attacker is to cause large-scale network outages, affecting Internet connectivity of individual Member States and possibly across the entire EU region that depends mostly on submarine cables. The sabotage/attack does not necessarily cause a full-service outage, due to the existing resilience of submarine and terrestrial cables, but significantly degrades connectivity services in the affected Member States. For this scenario, three escalation stages are defined.

Escalation stages

- *[Escalation 1: baseline]* **R1.1. Cable cut in territorial waters/EEZ of an EU Member State affecting at least two EU Member States.**

  In the baseline scenario, the cable cut takes place in territorial waters or the EEZ of an EU Member State but affects at least two Member States, thus including a cross-border dimension that requires some coordination between the affected Member States.

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

- *[Escalation 2]* **R1.2. Cable cut in territorial waters/EEZ of a third country affecting at least two EU Member States.**

  This scenario represents an escalation compared to R1.1, as the sabotage/attack is located in a non-EU third country. This is increasing transactional costs, such as transnational coordination between jurisdictions, for the affected EU Member States. In comparison, in R1.1, impacted EU Member States have full authority over the repair of the cable.

- *[Escalation 3]* **R1.3. Cable cut in high seas affecting at least three EU Member States.**

  This scenario represents an escalation compared to R1.2 in two ways. Firstly, the cable cut is located in international waters, where it is unclear who has legal jurisdiction and where it may take longer to recover the cable and repair it (notably in case of adverse weather conditions). Secondly, the higher number of affected Member States increases the coordination efforts between them.

Sub-scenarios

- **R1.4. Cutting off an entire island.**

  Three EU Member States are island nations (i.e., Cyprus, Ireland and Malta), making them more vulnerable to submarine cable sabotage/attacks due to the lack of cross-border terrestrial network connectivity. While the impact on the EU as a whole may be limited, severing all submarine cables of an island could result in its total isolation, with major consequences for its security, economic stability and social well-being.

- **R1.5. Cutting off an entire region.**

  Another sub-scenario is the cut-off of a region, which may be sub-national or involve more than one Member State. While the impact on the region itself may be similar to that of an island, usually it can be expected to be lower for the EU as a whole due to the availability of terrestrial backbone infrastructure (and associated capacity).

R2. Co-ordinated sabotage or attack on a cable landing site (beach manhole and/or landing station) (adapted from R6 in the Nevers Report).

Definition

A hostile actor manages to sabotage/attack the cable landing site through either a cyber intrusion into the landing station, or by physically sabotaging the beach manhole, or by destroying equipment at the cable landing station itself. The intent of the perpetrator can range from claiming ransom, to selling access to the submarine operating system to a hostile actor, or to directly disable the submarine cables connected to the landing site. This would not only affect Internet connectivity in the region where the landing site is located but also affect connectivity services across EU Member States connected to the submarine cables that land at the site.

Escalation stages

- *[Escalation 1: baseline]* **R2.1. Cyber intrusion into a cable landing station where cables land, affecting at least two EU Member States.**

  This baseline scenario considers only cybersecurity elements. A hostile actor manages to perform network intrusions inside the operating systems of all cables landing in a particular landing station. The actor can either directly exploit this access or create backdoors in the infrastructure and use or sell the backdoor access later for future cyber-attacks – for instance, eavesdropping on critical communications or service degradation.

- *[Escalation 2]* **R2.2. Sabotage of beach manholes where cables land, affecting at least two EU Member States.**

  As an escalation, the hostile actor manages to get access to the beach manholes (or intermediate manholes) and sever submarine cables using cutting tools (for example, an angle grinder) or explosives.

- *[Escalation 3]* **R2.3. Physical intrusion into a cable landing station where cables land, affecting at least two EU Member States, and destruction of equipment (including potentially the entire cable landing station).**

  While the barriers are higher, physically accessing a landing station to take control of the submarine cable system(s) and shutting it (them) down or destroying equipment represents a further escalation. In the worst case, a hostile actor could aim to destroy the entire landing station, where all active equipment and associated management systems are located. This would cause significant disruptions, as the landing station would have to be rebuilt, submarine line terminating equipment would have to be replaced, and the cables would have to be respliced and reconnected.

R3. Power cuts to cause a regional network outage (adapted from R9 in the Nevers Report)

Definition

A hostile actor targets the power grid in a certain region, causing a regional outage of the digital infrastructure including landing stations. The submarine cables linked to the affected landing stations remain operational for the first hours of the incident, using on-site battery backup systems. However, in the absence of a generator at the landing station and because the damage to the power grid is substantial, the power cut persists for several days. Since the heating, ventilation and air conditioning system is not connected to the backup power, the landing station is no longer cooled down and its temperature increases above the threshold for which the submarine line terminating equipment is designed to operate. Under this condition, the equipment enters into protection mode and the entire submarine cable system shuts down. This causes widespread connectivity outages in the EU Member State(s) connected to the affected cables.

Escalation stages

No escalation stages were defined for this scenario, as a prolonged grid outage would also affect all key nodes (for example, IXPs, data centres) directly or indirectly connected to the damaged submarine cable, and keeping the submarine cable infrastructure alone operational would not achieve any benefits. However, escalation can also be created by combining this scenario with others (see Section 5 on stress tests).

R4. Disruption of maintenance capability

Definition

From a fluctuation in market dynamics up to sabotage, disrupting maintenance capabilities (such as maintenance vessels and/or depots) will lead to a prolonged risk of outage, as it will increase the time to repair damaged submarine cables. While the impact of this scenario only materialises in the event of a cable cut, it has the potential to exacerbate the impact of the incident even for unintentional incidents caused by trawling and/or anchoring.

Escalation stages

- *[Escalation 1: baseline]* **R4.1. Market dynamics resulting in a temporary shortage of maintenance vessels in EU waters.**

  In the baseline scenario, instability in market conditions caused by increased demand, aging, relocation or ownership changes could lead to a temporary shortage of maintenance vessels within the EU maritime zones.

- *[Escalation 2]* **R4.2. Sabotage of a maintenance vessel serving EU waters or of a spares depot.**

  Deliberate sabotage of either a maintenance vessel operating in EU waters or a depot storing spare parts that are needed to repair damaged submarine cables in the EU constitutes an escalation. Such an incident would disrupt the ability to respond promptly even to accidental cable damage, potentially affecting multiple EU Member States.

- *[Escal. 3]* **R4.3. Co-ordinated sabotage of several maintenance vessels serving the EU or of several spares depots.**

  The launch of a coordinated sabotage/attack on several maintenance vessels and/or spares depots that support submarine cable infrastructures across the EU constitutes a further escalation. The coordinated nature of this event suggests strategic intent to disrupt repair capabilities at scale. The result could be widespread delays in restoring connectivity, increased exposure to cable failures and significant pressure on EU-wide crisis response mechanisms.

R5. Disruption of the supply chain

Definition

This scenario encompasses various causes that could disrupt the supply chain supporting submarine cable infrastructures. The disruption would affect the availability of key components and technical services. The supply chain disruption may be triggered by market dynamics, third-country interference or outright hostile actions. It may also be triggered by the imposition of an embargo on the EU (or on specific Member States) that blocks the delivery of critical parts. In more severe cases, compromised components may include embedded vulnerabilities (for example, backdoors) that enable remote sabotage or system shutdown. Consequences may include delayed repairs, reduced operational capacity and increased exposure to progressive system failures. It also limits the ability to increase capacity on existing systems or build new systems to address increasing capacity demand.

Escalation stages

- *[Escalation 1: baseline]* **R5.1. Market dynamics resulting in a temporary supply shortage of key components.**

  In the baseline scenario, fluctuations in global or regional markets lead to a temporary shortage of essential components for submarine cable systems or related infrastructure. Factors may include increased demand, manufacturing delays or logistical constraints.

- *[Escalation 2]* **R5.2. Third-country interference on a supplier of key components (including cyber espionage) (adapted from R2–4 in the Nevers Report).**

  An escalation would be the interference by a hostile State actor targeting suppliers of critical components, potentially through cyber espionage, regulatory pressure or covert influence. The aim may be to gain access to sensitive data, disrupt submarine cable supply chains or impose strategic control over the supplier.

- *[Escalation 3]* **R5.3. Block of supply (for example, embargo) or backdoor access to a system, enabling a malicious system shutdown.**

  A further escalation would arise if a hostile actor deliberately blocks the supply of critical submarine cable components (for example, through an embargo) or compromises components with hidden access points (backdoors) that allow for remote sabotage to trigger system failures or shutdowns across EU infrastructures.

R6. Unintentional cable damage caused by human activity

Definition

Unintentional physical damage to submarine cable infrastructures regularly occurs due to human activity such as bottom trawling, anchorage and dredging.

Escalation stages

There is no escalation stage to this scenario, as existing mitigating measures effectively reduce the likelihood of unintentional damage. However, escalation may arise when this scenario is combined with others (see Section 5 on stress tests).

R7. Natural events leading to physical damage on multiple cables or cable landing stations

Definition

Underwater natural events (such as seismic activity, slumping, undersea volcanoes or bottom currents) on a cable's route can lead to damage to the cable itself and/or active equipment (for example, repeaters). Impacts materialise, in particular, if there is insufficient redundant routing. Surface-level weather events such as cyclones, earthquakes or tsunamis may lead to damage to the dry plant. For example, cyclones or tsunamis may erode the beach landscape, exposing the cable and beach manhole, while earthquakes may directly damage the system.

Escalation stages

There is no escalation stage to this scenario, as existing mitigating measures against natural events will effectively reduce the likelihood of cable faults. However, escalation may arise when this scenario is combined with others (see Section 5 on stress tests).

Figure 4.5 below shows the different risk scenarios (and sub-scenarios), as well as the threats, vulnerabilities and dependencies linked to each of them.

Figure 4.5: Risk scenarios and sub-scenarios [Source: Analysys Mason, 2025]

	Risk (sub-)scenario	Threats	Vulnerabilities	Dependencies
R1. Coordinated physical sabotage or attack on submarine cable (R6 in the Nevers Report)				
Escal. 1	**R1.1.** Cable cut in territorial waters/ EEZ of an EU Member State affecting at least two EU Member States	**T1.** Cable cuts in territorial waters **T2.** Cable cuts in EEZ	**V14.** Exposed cable at fishing/anchoring depth **V15.** Lack of cable armouring at fishing/anchoring depth **V16.** Lack of surveillance/advanced monitoring systems	**D19.** Lack of a plan to respond to an emergency situation **D20.** Lack of centralised reporting of physical and/or cyber incidents **D21.** Lack of a coordination entity in each Member State or between countries to respond to a submarine cable incident or emergency situation **D22.** Lack of information sharing between public entities from different Member States **D23.** Lack of public–private coordination
Escal. 2	**R1.2.** Cable cut in territorial waters/ EEZ of a third country affecting at least two EU Member States	*Same as **R1.1.***	*Same as **R1.1.***	*Same as **R1.1.** with additions:* **D17.** Long process to obtain permits **D18.** Lack of jurisdiction for incidents in EEZ and high seas
Escal. 3	**R1.3.** Cable cut in high seas affecting at least three EU Member States	**T3.** Cable cuts in high seas	**V16.** Lack of surveillance/advanced monitoring systems	*Same as **R1.2.** with additions:* **D9.** US dependency **D10.** UK dependency **D11.** Chinese dependency **D12.** Russian dependency **D13.** Cables located in geopolitically unstable areas **D15.** Chokepoints

	Risk (sub-)scenario	Threats	Vulnerabilities	Dependencies
N/A	**R1.4**. Cutting off an entire island	*Same as **R1.1.** with additions:* **T3.** Cable cuts in high seas **T4.** Cable cuts in backhaul **T5.** Damage to/destruction of beach manhole **T6**. Physical security breach at cable landing station **T7**. Damage to/destruction of cable landing station	**V1**. Insufficient physical security at beach manhole **V2**. Insufficient physical security at cable landing station or NOC **V3**. Insufficient physical security at depots **V4.** Lack of a depot backup location **V5**. Exact position of cable, depots and cable landing station available in the public domain **V16**. Lack of surveillance/advanced monitoring systems	*Same as **R1.1.** with additions:* **D10**. UK dependency **D13**. Cables located in geopolitically unstable areas **D14.** Lack of route diversity **D15**. Chokepoints **D17.** Long process to obtain repair permit
N/A	**R1.5**. Cutting off an entire region	*Same as **R1.4.***	*Same as **R1.4.***	*Same as **R1.4.** with additions:* **D19**. Lack of a plan to respond to an emergency situation **D20.** Lack of centralised reporting of physical and/or cyber incidents **D21**. Lack of a coordination entity in each Member State or between countries to respond to a submarine cable incident/emergency situation **D22.** Lack of information sharing between public entities from different Member States **D23**. Lack of public–private coordination

	Risk (sub-)scenario	Threats	Vulnerabilities	Dependencies
R2. Coordinated sabotage or attack on cable landing site (beach manhole and/or landing station) (adapted from R6 in the Nevers Report)				
Escal. 1	**R2.1**. Cyber intrusion into a cable landing station where cables land, affecting at least two EU Member States	**T6**. Physical security breach at cable landing station **T7**. Damage to/destruction of cable landing station **T14**. Network intrusion/intrusion into operating system **T15**. Insider threat **T16**. Cybersecurity attack on an M(M)SP or other third-party service provider	**V7**. Insufficient cybersecurity in network management **V8**. Insufficient cybersecurity of network equipment **V9**. Insufficient cybersecurity of end-user devices	**D19**. Lack of a plan to respond to an emergency situation **D20.** Lack of centralised reporting of physical and/or cyber incidents **D21**. Lack of a coordination entity in each Member State or between countries to respond to a submarine cable incident/emergency situation **D22.** Lack of information sharing between public entities from different Member States **D23**. Lack of public-private coordination
Escal. c	**R2.2**. Sabotage of beach manholes where cables land, affecting at least two EU Member States	**T5**. Damage to/destruction of beach manhole	**V1**. Insufficient physical security at beach manhole	*Same as **R2.1.** with additions:* **D16**. Dependency on technical expertise
Escal. 3	**R2.3**. Physical intrusion into a cable landing station where cables land, affecting at least two EU Member States, and destruction of equipment (including potentially the entire cable landing station)	**T6**. Physical security breach at cable landing station **T7**. Damage to/destruction of cable landing station	**V2**. Insufficient physical security at cable landing station or NOC **V5**. Exact position of cable, depots and cable landing station available in the public domain	*Same as **R2.1.***
R3. Power cuts to cause a regional network outage (R9 in the Nevers Report)				
N/A	N/A	**T8**. Power outage due to damage to the grid/transformer	**V6**. Lack of backup power supply at cable landing station	*Same as **R2.1.** with additions:* **D8**. Power supply dependency

	Risk (sub-)scenario	Threats	Vulnerabilities	Dependencies
R4. Disruption of maintenance capability				
Escal. 1	**R4.1**. Market dynamics resulting in a temporary shortage of maintenance vessels in EU waters	**T11**. Blockage of access to vessels **T12**. Damage to/destruction of maintenance vessels		**D6**. Lack of maintenance capability in the EU **D7.** Lack of EU shipyard capacity for building new vessels **D16**. Dependency on technical expertise
Escal. 2	**R4.2**. Sabotage of a maintenance vessel serving EU waters or a spares depot	**T9**. Blockage of access to depot **T10.** Damage to/destruction of depot **T12**. Damage to/destruction of maintenance vessels	**V3**. Insufficient physical security at depots **V4.** Lack of a depot backup location **V5**. Exact position of cable, depots and cable landing station available in the public domain	**D6**. Lack of maintenance capability in the EU **D7**. Lack of EU shipyard capacity for building new vessels
Escal. 3	**R4.3**. Co-ordinated sabotage of several maintenance vessels serving the EU or of several spares depots	*Same as **R4.2.***	*Same as **R4.2.***	*Same as **R4.2.** with additions:* **D19**. Lack of a plan to respond to an emergency situation

	Risk (sub-)scenario	Threats	Vulnerabilities	Dependencies
R5. Disruption of supply chain				
Escal. 1	**R5.1.** Market dynamics resulting in a temporary supply shortage of critical components	**T13.** Physical attack on the supply chain causing disruption	**V4.** Lack of a depot backup location **V5.** Exact position of cable, depots and cable landing station available in the public domain	**D1.** Supplier dependency **D3.** Lack of components in the market due to high demand/insufficient supply **D4.** Lack of standardisation in submarine system components **D5.** Shifting market demand from telecoms towards a hyperscaler (data centres/AI) business model **D9.** US dependency
Escal. 2	**R5.2.** Third-country interference on a supplier of essential components (including cyber espionage) (R2–4 in the Nevers Report)	**T14.** Network intrusion/intrusion into operating system **T15.** Insider threat **T16.** Cybersecurity attack on an M(M)SP or other third-party service provider **T17.** Cybersecurity attack on the supply chain causing disruption		**D2.** Lack of components due to nation state influence/control of supplier **D19.** Lack of a plan to respond to an emergency situation
Escal. 3	**R5.3.** Block of supply (for example, embargo) or backdoor access to the system, enabling malicious system shutdown	*Same as **R5.2.***	**V7.** Insufficient cybersecurity in network management **V8.** Insufficient cybersecurity of network equipment **V9.** Insufficient cybersecurity of end-user devices	**D1.** Supplier dependency **D2.** Lack of components due to nation state influence/control of supplier

	Risk (sub-)scenario	Threats	Vulnerabilities	Dependencies
R6. Unintentional cable damage caused by human activity				
N/A	N/A	**T1**. Cable cuts in territorial waters **T2.** Cable cuts in EEZ **T3.** Cable cuts in high seas **T4.** Cable cuts in backhaul **T5.** Damage to/destruction of beach manhole **T7.** Damage to/destruction of cable landing station **T18.** Fishing (cable cut) **T19.** Anchors (cable cut) **T20.** Civil works and dredging (cable cut) **T21.** Deep sea mining (cable cut) **T22**. Misconfiguration of network	**V10**. Lack of education on submarine cables for the fishing industry **V11**. Lack of protection area around the submarine cable route in territorial waters **V13**. Unreliable network equipment **V14.** Exposed cable at fishing/ anchoring depth **V15.** Lack of cable armouring at fishing/anchoring depth **V16**. Lack of surveillance/advanced monitoring systems	**D13**. Cables located in geopolitically unstable areas **D17.** Long process to obtain repair permit **D18.** Lack of jurisdiction for incidents in EEZ and high seas **D20.** Lack of centralised reporting of physical and/or cyber incidents **D21**. Lack of a coordination entity in each Member State or between countries to respond to a submarine cable incident/emergency situation **D22.** Lack of information sharing between public entities from different Member States **D23**. Lack of public–private coordination

	Risk (sub-)scenario	Threats	Vulnerabilities	Dependencies
R7. Natural events leading to physical damage on multiple cables or cable landing stations				
N/A	N/A	**T1**. Cable cuts in territorial waters **T2.** Cable cuts in EEZ **T3.** Cable cuts in high seas **T4.** Cable cuts in backhaul **T5.** Damage to/destruction of beach manhole **T7**. Damage to/destruction of cable landing station **T23.** Undersea seismic activity **T24.** Undersea volcanos **T25.** Slumping **T26.** Beach erosion **T27.** Bottom current **T28**. Adverse weather events	**V12**. Cables located in geographically unstable areas **V13**. Unreliable network equipment	**D8**. Power supply dependency **D14.** Lack of route diversity **D17.** Long process to obtain repair permit **D18.** Lack of jurisdiction for incidents in EEZ and high seas **D20.** Lack of centralised reporting of physical and/or cyber incidents **D21**. Lack of a coordination entity in each Member State or between countries to respond to a submarine cable incident/emergency situation **D22.** Lack of information sharing between public entities from different Member States **D23**. Lack of public–private coordination

5. STRESS TEST GUIDANCE

As stated in Recommendation (EU) 2024/779, ([26]) "Member States should be encouraged to make entities operating submarine cable infrastructure subject to regular stress testing", based on common principles at Union level.

This section aims to provide guidance to Member States and critical infrastructure operators on how to develop stress tests and apply resilience indicators for submarine cable infrastructures.

5.1. Methodology and stress test for risk scenarios

Stress tests have multiple definitions based on the context and purpose for which they are applied. For this report, and in line with work done in the energy sector (see below), a stress test is defined as a dedicated and targeted assessment of the resilience of critical infrastructure and the entity that operates it based on extreme, but realistic, pre-defined scenarios.

The stress test methodology developed in this report aligns with i) Strategic Recommendation 8 of the Nevers Report, ([27]) which specifically emphasises the need to extend physical stress testing to digital infrastructure, ii) the stress test methodology developed for the energy sector in the context of the 2022 Critical Infrastructure Council Recommendation (non-public document), iii) ENISA's 2025 Handbook for Cyber-Stress Tests, ([28]) and iv) a scenario developed by the Hybrid Centre of Excellence in 2025 (non-public).

The methodology developed for the energy sector and ENISA's Handbook constitute the main points of reference. From the risk scenarios identified in Section 4.3 (also referred to as 'injects', in line with the terminology used for the energy sector), this section selects the ones with a potentially high impact (regardless of likelihood) and groups them into a more aggregated approach, where various risk scenarios are grouped in three escalation stages.

While the full stress test methodology applied to the energy sector is not public (as mentioned above), limited explanations on the similarities and differences between both approaches are outlined in Figure 5.1.

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

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

([28]) ENISA (2025), *Handbook for Cyber Stress Tests*.

Figure 5.1: Comparison of stress test methodology for the energy sector and for submarine data cables [Source: Analysys Mason, 2025]

Methodology for the energy sector	Methodology for submarine data cables
Scope: direct, intentional man-made risks resulting from malicious acts	Scope: direct and indirect risks (for example, supply chain, market), including unclear attribution and potentially unintentional damage through human activity (for example, fishing accidents) as well as natural events (Scenarios R6 and R7 above)
Identification of attack vectors and modus operandi	Attack vectors and modus operandi incorporated into a broader overview of threats, vulnerabilities and dependencies
Risk building block injects	Risk scenarios/injects
Broader background scenario with escalation stages, in addition to risk injects	Escalation stages already embedded in risk scenarios/injects, then grouped into a more aggregated approach to achieve both higher modularity and less complexity and repetition
Breakdown per energy subsector as defined in the Annex of the CER Directive	No subsectors for digital infrastructure defined in the Annex of the CER Directive
Breakdown of entities per category, as defined in the Annex of the CER Directive	Operation of a submarine data cable, independent of the entity defined in the Annex of the CER Directive

Below, a stress test approach is proposed for the risk scenarios identified in Section 4.3. They have been grouped into three different escalation stages, to reflect the escalating impact (see Figure 5.23).

Figure 5.23: Stress test stages [Source: Analysys Mason, 2025]

Stage	Risk scenario/sub-scenario
Stage 1	R1.1. Cable cut in territorial waters/EEZ of an EU Member State affecting at least two EU Member States
	R2.1. Cyber intrusion into a cable landing station where cables land that affect at least two EU Member States
	R4.1. Market dynamics resulting in a temporary shortage of maintenance vessels in EU waters
	R5.1. Market dynamics resulting in a temporary supply shortage of key components
Stage 2	R1.2. Cable cut in territorial waters/EEZ of a third country affecting at least two EU Member States
	R2.2. Sabotage of beach manholes where cables land that affect at least two EU Member States
	R4.2. Sabotage of a maintenance vessel serving EU waters or a spares depot
	R5.2. Third-country interference on a supplier of critical components (including cyber espionage) (R2–4 in the Nevers Report)
Stage 3	R1.3. Cable cut in high seas affecting at least three EU Member States
	R2.3. Physical intrusion into a cable landing station where cables land, affecting at least two EU Member States, and destruction of equipment (including potentially the entire cable landing station)
	R3. Power cuts to cause a regional network outage (R9 in the Nevers Report)
	R4.3. Coordinated sabotage of several maintenance vessels serving the EU or of several spares depots
	R5.3. Block of supply (for example, embargo) or backdoor access to the system, enabling malicious system shutdown
Optional	R1.4. Cutting off an entire island
	R1.5 Cutting off an entire region
	R6. Unintentional cable damage caused by human activity
	R7. Natural events leading to physical damage on multiple cables or cable landing stations

Member States may select from the proposed stages in order to conduct the stress tests but are encouraged to at least include the baseline Stage 1. They may adapt the scenarios and incorporate elements specific to their national context (for example, island scenarios), in addition to the general EU-wide risk scenarios. Member States may also choose to include higher-impact scenarios than the ones proposed. They are encouraged to explore systemic risks by also covering the supply chain dimension and interdependencies. For instance, the impact of an incident may be amplified when an organisation (1) depends on the affected service, and (2) lacks alternative services. This type of risk becomes particularly critical at the societal level when multiple organisations rely on the same service, as a disruption can lead to widespread, simultaneous effects.

Member States may also consider expanding the risk scenarios to reflect the cumulative effects of multiple, possibly smaller, incidents. These may include incidents affecting individual organisations as well as supply chain disruptions occurring in parallel with the main scenario. Furthermore, Member States are encouraged to balance the focus across different types of incidents, including system failures, human error, malicious acts and natural phenomena.

In an environment where intentionality and attrition cannot always be confirmed, the impact of an incident caused by accidental or natural events may be comparable to the impact of an incident caused by sabotage.

5.2. Practical considerations for implementation

Authorities responsible for conducting stress tests for submarine cable infrastructures may refer to the Handbook for Cyber Stress Tests, published by ENISA in May 2025. ([29]) The handbook outlines common characteristics of stress tests, provides a step-by-step methodology, includes practical examples and explains how such tests can be implemented at EU level. In particular, it proposes the following five steps for conducting the stress tests:

- **Scope and objectives** – The scope and objectives of the stress test are defined by choosing the sector, the target entities and infrastructure, and the high-level risk scenarios. In this step, stakeholders who can support and help design the stress test are identified.
- **Design** – The authority designs the stress test by choosing the methodology, refining the scenario and developing the resilience metrics that are linked to the stress test objectives.
- **Execution** – The authority engages with the entities to execute the stress test, providing guidance and explanation about the objectives of the test, the overall timeline and planning, and how results will be analysed and gaps followed up.
- **Gap analysis** – Data analysis is used to identify gaps, weaknesses and areas for improvement, for the individual entities and/or the sector overall. Stress test results are assessed both qualitatively and quantitively against the predefined resilience metrics.
- **Conclusion** – In the final step, authorities report the findings from the test. If needed, they issue recommendations for individual entities or sector-wide recommendations. Authorities then oversee that such recommendations are implemented and draw on lessons learned.

As part of the design phase for a submarine cable stress test, a set of indicators may be proposed to measure the level of preparedness, resilience and the impact of the scenarios, ultimately evaluating an entity's ability to withstand and recover from disruptions. These indicators, linked to the objectives of the stress test, can be qualitative or quantitative, and are designed to provide a structured and measurable framework for assessing performance and resilience under stress. They help to identify weaknesses, assess the effectiveness of mitigation measures and point to areas for improvement. Resilience indicators aim to capture both the technical and organisational dimensions of preparedness, incident response and recovery. Example indicators could include the following:

- time to detect an incident
- time to respond to and/or recover from an incident
- level of sophistication of preventative measures
- degree of service degradation/loss of functionality.

Resilience indicators would require the development of appropriate thresholds to measure and evaluate the results from the stress test, which may differ across Member States and are therefore not elaborated in this report. To increase comparability across Member States, EU-wide standardisation – such as scenario-specific key performance indicators, templates and other tools – could be developed following the initial round of stress tests.

[29] ENISA (2025), *Handbook for Cyber Stress Tests*.