



Funded by
the European Union
NextGenerationEU



Powered by



LUISS 
Research Center
for International
and Strategic Studies

OCTOBER.2026

The underwater dimension

New threat and reaction scenarios for the country

In collaboration with



The underwater dimension

New threat and reaction scenarios for the country

Contributors

Raffaele Marchetti, Alessandro Celestra, Manfredi Valeriani, Denise Danili, Antonio Leandro, Daniela Irrera, Carolina Polito, Gabriele Marchionna, Giacomo Leccese, Ivan Fraternali, Lorenzo di Stefano, Claudio Passalacqua

Table of Contents

<i>Executive Summary</i>	5
1. Mapping of Italian strategic underwater infrastructures	6
1.1 Definition of underwater infrastructure and strategic criteria	6
1.2 Types and architecture of underwater critical infrastructures	7
1.3 The main national networks and backbones	9
1.4 Choke points and areas of greatest vulnerability	14
2. Regulatory and jurisdictional perimeter of the underwater dimension	16
2.1 The sovereignty and jurisdiction of the coastal state	16
2.2 The grey areas of the high seas: limits of enforcement mechanisms and regulatory gaps	17
2.3 Other relevant international instruments and liability profiles	19
2.4 The Italian regulatory framework: Law 9/2026 and the new competences of the Navy..	19
2.5 Ideas for cooperation and strategic projection	21
3. Risks and threats to subsea infrastructure	23
3.1 Scope of analysis	23
3.2 Undeliberate threats.....	25
3.3 Deliberate and hybrid threats.....	27
3.4 Vectors and modes of action.....	31
3.5 Risk mapping.....	37
4. Defense Solutions and Protection Models.....	40
4.1 Prevention, surveillance and deterrence measures in the underwater context	40
4.2 Passive protection and infrastructure resilience	42
4.3 Response and Recovery Following Disruption	44
4.4 The Repair Process	45
5. Foreign experiences	47
5.1 United States	47
5.2 France	47
5.3 Japan	47
5.4 Australia.....	48
5.5 Sweden	48
5.6 United Kingdom	48
5.7 Ireland.....	48

5.8 Israel	49
5.9 China.....	49
5.10 Egypt.....	49
5.11 Turkey.....	50
6. The underwater dimension to 2050: four futures for Italy	51
6.1 Why look to 2050, and how.....	51
6.2 What will happen anyway: the predetermined elements.....	51
6.3 The two critical uncertainties.....	52
6.4 What the scenarios teach: robust measures and contingency measures	56

Index of Figures

Figure 1. Telecom submarine cable system.....	7
Figure 2. Subsea infrastructure system for the transport of gas and hydrocarbons	9
Figure 3. Submarine Cable Map.....	10
Figure 4. Subsea Gas System.....	11
Figure 5. Distribution of maritime spaces according to UNCLOS.....	17
Figure 6: Future scenarios for Italy.....	53

Table Index

Table 1. Risk matrix for subsea infrastructure.....	38
Table 2. Risk - Impact Matrix.....	39

Executive Summary

The underwater dimension has become one of the primary fronts of national security, and the Mediterranean today represents one of the most vulnerable and strategic theaters in the world. Italy, due to its geographical position and concentration of landing points in Sicily, Puglia and Liguria, is one of the states most exposed to accidental risks and hybrid threats, with a dependency profile that makes the operational continuity of underwater infrastructures a national strategic asset. Today's threats are reduced compared to potential future threats due to at least three fundamental elements: 1) the proliferation of low-cost weapons such as marine drones, 2) the increase in international tensions; 3) the preparation of future threats (mapping of infrastructures, pre-positioning of latent tools, etc.) that could have a significant impact in the event of future conflicts.

The new responsibilities introduced by Law 9/2026 assign the Navy a central role in surveillance, deterrence and enforcement in the underwater dimension, including control activities in inland waters, in the territorial sea and on the continental shelf, as well as the prevention of hostile underwater navigation. In addition to these functions, there is the task of cooperation with allied navies and with the Agency for the Safety of Underwater Activities (ASAS).

The most frequent risk for Italian submarine infrastructures is not direct sabotage, but accidental accidents (anchors, fishing nets, seabed instability), often indistinguishable in the early stages from potential hybrid attacks. This ambiguity requires the ability to quickly recognize, secure coastal nodes and control access to sensitive areas immediately after an interruption. The underwater dimension also remains characterized by a strong physical opacity: this makes it essential to develop an advanced *Underwater Domain Awareness* (UDA) based on active/passive sonar, MAD, AUV and ROV systems, integrated into an interagency command and control framework that allows an accurate assessment of anomalies and effective *deterrence by detection*.

In addition, the possibility of state actors or proxies hitting critical infrastructures in shallow waters, interfering with cable-laying vessels or conducting cyber pre-positioning operations makes it necessary to develop an active posture also in the logistical, cyber and geoeconomic dimensions. The protection of repair ships, the management of maritime *choke points* and the coordination with private operators and port authorities thus become decisive components of national underwater security.

Finally, the international dimension is an integral part of the mission: the infrastructures that insist on the Mediterranean depend on the stability of areas such as the Red Sea, the Suez Canal and the Eastern Mediterranean. It will therefore be necessary to contribute to a Euro-Atlantic underwater security architecture that integrates awareness, resilience and response capabilities with NATO, the EU and regional partners.

In this context, the protection of the underwater dimension is not only a technical challenge, but a strategic task that requires a combination of operational superiority, inter-institutional cooperation and anticipation, so that Italy preserves its function as a critical hub of energy and digital security in the Mediterranean.

1. Mapping of Italian strategic underwater infrastructures

1.1 Definition of underwater infrastructure and strategic criteria

Underwater infrastructure refers to the set of essential structures and systems located on or below the seabed, crucial for a variety of operations including communications, energy production and transport, transport and defense. This category therefore includes submarine fiber optic cables, which today carry about 99% of international communications, power cables for the transmission of energy between regions and countries, oil and gas pipelines, offshore renewable energy installations, marine research and surveillance facilities, as well as transport infrastructures with submerged foundations such as underwater tunnels. The strategic nature of these infrastructures is not exclusively an intrinsic technical property, it is rather the result of a political-institutional assessment that reflects economic priorities, perceived vulnerabilities and national security objectives. It is divided into three distinct levels: functional, systemic and security/geopolitical.

On a functional level, an underwater infrastructure is strategic when it enables or conditions the provision of services essential for the functioning of the State. The criticality does not depend on the technical nature of the asset itself, but on its enabling role with respect to functions such as the continuity of communications, or the security of energy supplies. The interruption of these functions would in fact compromise the operational continuity of the country. A fiber optic cable that carries commercial internet traffic, for example, can become strategic when it also enables military communications or control systems of critical terrestrial infrastructures. From a systemic point of view, strategic is instead measured in terms of substitutability, redundancy and cascading effects. In defining this dimension, three indicators are particularly relevant: low substitutability, which occurs when alternative routes are scarce or when the reallocation of traffic would require times incompatible with the continuity of essential services; low redundancy, which manifests itself in the concentration of numerous routes on the same sea corridors or on a limited number of landing points, increasing the probability that a single event will produce extensive impacts; and high interdependence, whereby an energy outage can cascade into digital networks and other critical services, multiplying the effect of the initial damage. Finally, from a security and geopolitical point of view, infrastructures with dual-use value are of particular importance, as well as those assets that contribute to consolidating the country's role as a Mediterranean connectivity hub and hub of global data and energy networks, projecting it as a bridge between Europe, Africa, the Middle East and Asia.

It should be noted that, although submarine infrastructure can be targets of malicious actions, the most frequent incidents remain accidental in nature such as commercial fishing and navigation activities or natural phenomena such as earthquakes and underwater landslides¹. However, the events recorded in recent years, particularly in the Baltic Sea area (Nordstream 1&2 - 2022, Baltconnector - 2023, BCS East-West Interlink data cable - 2024),² signal an escalation of deliberate hostile actions that requires a reconsideration of the overall risk profile. To further complicate the picture,

¹ European Commission Joint Research Center (2025), "Subsea cables: how vulnerable are they and can we protect them?"

² Lindholm, R. (2025, March 24). Mapping undersea infrastructure attacks in the Baltic Sea. Wilson Center.

the repair of a submarine cable or landing station is a complex, time-consuming operation that depends on an extremely small number of specialized vessels available worldwide: a coordinated attack against the main submarine infrastructure would therefore have a potential major systemic impact on national security.

1.2 Types and architecture of underwater critical infrastructures

Starting from the general definition of underwater infrastructures, it is possible to identify some specific types³. Those of greatest strategic importance are undoubtedly communication and energy infrastructures. The first category includes submarine cables for telecommunications. The submarine cable system for telecommunications consists of a submerged part (*wet plant*) and a land part (*dry plant*), both essential for the continuity of transmission⁴. The submerged component includes the fiber optic cable, repeaters that amplify the signal at regular intervals of about 100 km along the ocean floor, and in some cases branch devices that allow ramifications to multiple destinations. The land part, on the other hand, includes the coastal landing point (*beach manhole*) and the landing stations, which house the terminal equipment, power systems and devices connecting with the land network. The cables are laid by specially designed vessels, the cable layers, in a process that can take one to three years from planning to commissioning. In deep water, the cables are laid directly on the seabed. Near the coast, they are buried in trenches using specialized ploughs and then lined with galvanized steel reinforcement for protection purposes.

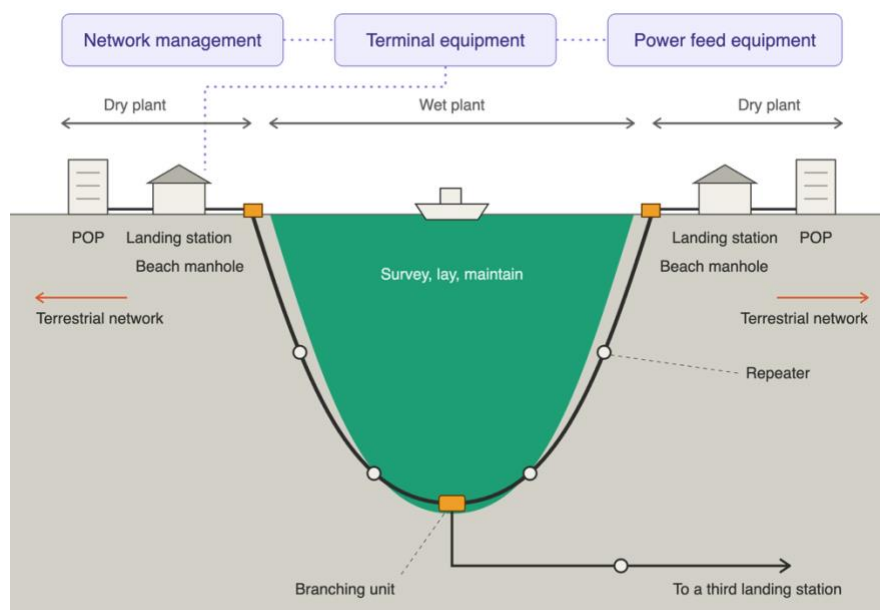


Figure 1. Telecom submarine cable system⁵

³ Cassetta, M. (2024). Threats to national underwater critical infrastructures. *Maritime Review* September-October 2024

⁴ Swinhoe, D. (2021). What is a submarine cable? subsea fiber explained. *Data Center Dynamics*. Retrieved June, 25, 2023

⁵ Adapted from: Jill C. Gallagher (2022), "Undersea Telecommunication Cables: Technology Overview and Issues for Congress," U.S. Congressional Research Service, p. 5, <https://crsreports.congress.gov/product/pdf/R/R47237>.

A modern submarine cable system is usually divided into three overlapping layers: the physical layer (the cable and its supporting infrastructure), the logical layer (the Network Management Systems that remotely monitor and control data transmission) and the informational layer (the data packets conveyed along the system). The interweaving of these three layers determines the continuity of global communications and, at the same time, multiplies the attack surfaces that can potentially be exploited by hostile actors.

Another category of infrastructure is represented by submarine power cables, which have taken on an increasing role in the configuration of the European energy system, performing essential functions for the integration of offshore renewable energy, the creation of interconnection between countries and the stabilization of electricity markets through cross-border trade. Cables of this type can transmit energy in alternating current (Alternating Current AC/ High Voltage Alternating Current - HVAC) or in high voltage direct current (HVDC). For short distances (less than about 80km), AC technology is cheaper, while for longer routes it becomes necessary to use HDVC, which allows hundreds of kilometers to be covered with fewer losses. Similarly to telecommunications cables, the submarine power cable infrastructure has a submerged segment (cable, protection systems, any reinforcements) and an underground segment with converter and transformation stations, which are critical nodes for interconnection with the national electricity grid. The installation of these cables is preferably done by burying them in the seabed using underwater ploughs, in order to reduce the risk of damage.

Finally, the last type of underwater infrastructure to consider is that of gas and hydrocarbon pipelines. In the energy sector, subsea pipelines for the transport of gas and hydrocarbons represent infrastructures of primary importance for national energy security. For these infrastructures, the submerged segment includes the main pipeline, generally made of high-strength steel, covered with protective anti-corrosion layers, thermal insulation to prevent the formation of hydrants and, frequently, metal reinforcements to ensure stability on the seabed. Along the route there may also be underwater collection structures (*manifolds*) and *vertical risers* that connect the seabed to offshore platforms or floating production units. In deep water, the pipeline is laid directly on the seabed. In coastal areas, on the other hand, it is buried by digging trenches. The integrity of the system is monitored through flow pressure sensors and digital supervision and control platforms (SCADA), which allow remote management and the identification of anomalies.

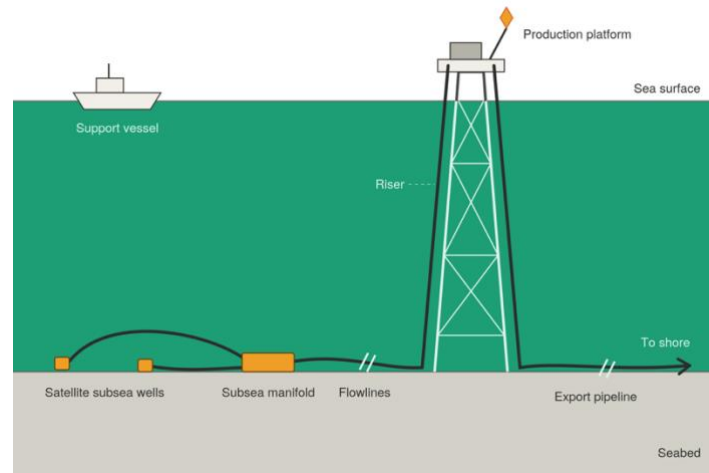


Figure 2. Subsea infrastructure system for the transport of gas and hydrocarbons⁶

1.3 The main national networks and backbones

The Italian underwater telecommunications network is strongly polarized around three main nodes, each with a distinct geographical function in the international connectivity system. Sicily is the main national hub, positioning itself as a convergence point for the intercontinental backbones that connect Europe to the Middle East, Asia and sub-Saharan Africa. AAE-1 (Asia Africa Europe 1), which connects Hong Kong to Europe through the Red Sea and the Eastern Mediterranean, and 2Africa, the next-generation African perimeter cable co-financed by Meta and other *hyperscalers* (Google, Amazon, Microsoft), ⁷destined to become one of the highest capacity systems in the world, transit or land through Sicily.

Sicily's position in the central Mediterranean basin transforms it into an obligatory transit node for data flows between Europe and the eastern and southern regions of the globe. Also in the south of the country, we find another important hub, that of Bari which performs the function of the main Adriatic entry point, with a strategic role for connections to the Balkans, the Middle East and the Black Sea, helping to position Italy as a digital *gateway* on the Adriatic-Ionian axis. Genoa and Savona are the main northern Tyrrhenian hubs, with connections to France, Spain and North Africa through the BlueMed system and other cables that transit the Ligurian Sea.

⁶ Adapted from: Control Solutions for Multiphase Flow: Linear and nonlinear approaches to anti-slug control - Scientific Figure on ResearchGate. Available from:

⁷ Salgado, R. (2024), Undersea Cables, Hyperscalers, and National Security, Hoover Institution, Stanford University, Aegis Series Paper No. 2304

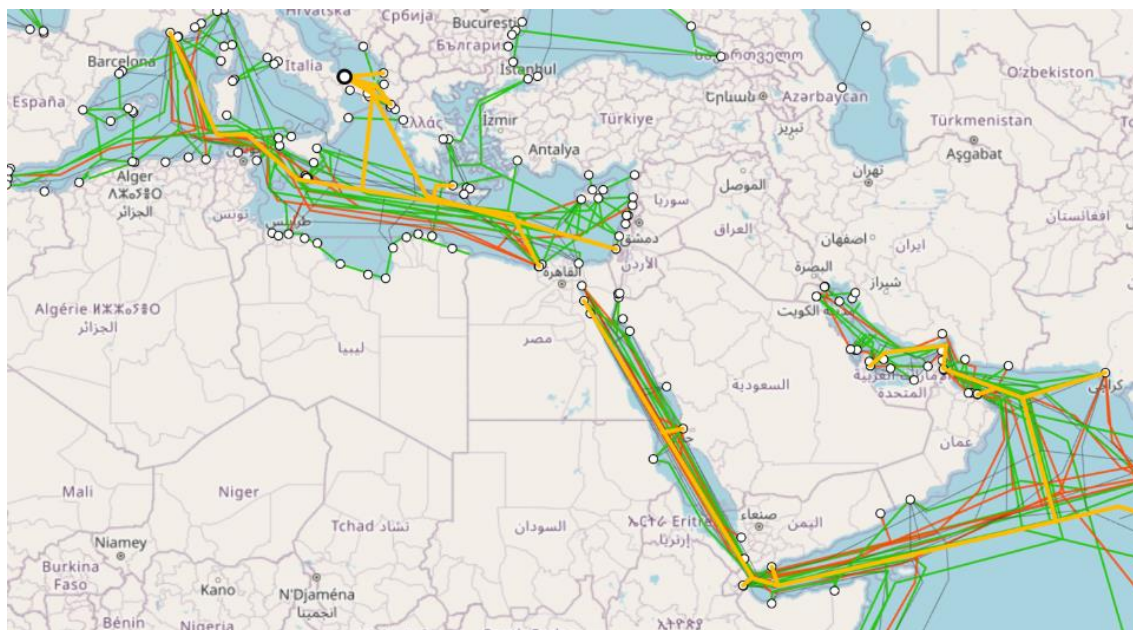


Figure 3. Submarine Cable Map⁸

The structure is therefore highly polarized with important direct implications on the risk profile of the system. The concentration of landing points in a few geographical areas, Sicily and Puglia in the first place, determines the existence of *territorial single points of failure*; damage or interruption in one of these areas would have immediate effects that would be difficult to mitigate on the entire international connectivity of the country.

As far as the gas system is concerned, the Mediterranean energy system develops mainly along the north-south axis, with Italy playing a dual role, that of the final market for supplies from Africa and the Middle East and that of a potential transit platform towards central-northern Europe.

The main gas infrastructures that concern the Italian underwater dimension are:

2. **Transmed (Trans-Mediterranean pipeline):** historical axis of Algerian gas imports through Tunisia and the Strait of Sicily, with a landing point right on the island. Transmed has been the country's main supply artery for decades and continues to maintain a structural role in the national energy system, also accentuated by the growing centrality of Algeria as a gas supplier following the War in Ukraine and the consequent cessation of imports from Russia.
3. **Greenstream;** an undersea pipeline that connects Libya to Italy through the Strait of Sicily, bringing gas from the Wafa field and Libyan coastal installations to southern Sicily. Its operation is conditioned by Libyan political stability, making it an asset with high geopolitical vulnerability.
4. **TAP (Trans Adriatic Pipeline):** the most recently built infrastructure that brings Azerbaijani gas from Azerbaijan through Georgia, Turkey and Greece to the landing place in Puglia. The TAP represents the terminal segment of the Southern

⁸ Telegeography (2026), Submarine Cable Map

Gas Corridor (SGC) and is one of the strategic axes for the diversification of Italian and European supplies.

Overall, the geography of the Italian gas system shows a dual dependence, both on physical infrastructures crossing maritime areas with a high degree of instability or under the sovereignty of third countries, and on maritime corridors, primarily the Straits of Sicily and Otranto, which constitute geographical bottlenecks for the entire supply chain.



Figure 4. Subsea Gas System⁹

The weight of the LNG carrier in the national mix makes this exposure anything but marginal. In 2024, LNG accounted for about 25% of Italy's gas imports, equal to about 14.6 billion cubic meters, a share that rose to about 30% in the first half of 2025¹⁰. The flows come from a small number of liquefaction basins: in 2024, Qatar supplied about 45% of imported LNG (≈ 6.6 billion cubic meters), the United States about 35% (≈ 5.2 billion cubic meters) and Algeria about 14% (≈ 2 billion cubic meters); during 2025, the United States overtook Qatar as the first supplier, accounting for around 45% of deliveries¹¹. These flows converge on five regasification plants whose geography is not neutral with respect to Mediterranean bottlenecks: three plants gravitate around the Tyrrhenian-Ligurian basin (Panigaglia, OLT Livorno, FSRU Piombino), two on the northern Adriatic (Adriatic LNG/Porto Levante and the FSRU of Ravenna, operational from April 2025). Out of a national regasification capacity of the order of 28 billion

⁹ Adapted from: Agenzia Nova (2022), Energy: here is the new map of gas flows in Italy

¹⁰ U.S. Department of Commerce, International Trade Administration, *Italy Energy – Liquefied Natural Gas (LNG)*, Market Intelligence, 2025, <https://www.trade.gov/market-intelligence/italy-energy-liquefied-natural-gas-lng>

¹¹ S&P Global Commodity Insights, *Italy's LNG regasification capacity growth central to Russian gas displacement: Snam*, 17 December 2024, <https://www.spglobal.com/energy/en/news-research/latest-news/natural-gas/121724>

cubic meters per year, the two Adriatic terminals account for more than half, and Porto Levante alone covers about 15% of national gas demand¹².

It is the combination of the direction of origin and the landing basin that determines which *choke point* is binding. Incoming cargoes from Gibraltar (United States and, more generally, the Atlantic basin) reach the Tyrrhenian terminals without transiting either through the Strait of Sicily or that of Otranto; to serve the Adriatic terminals they are instead obliged to cross both. Cargoes of western Mediterranean origin (Algeria) serve the Tyrrhenian terminals without constraints but meet the Strait of Sicily if directed to the Adriatic. Cargoes of Middle Eastern or Levantine origin (Qatar, Egypt) enter from Suez and must cross the Strait of Sicily to serve the Tyrrhenian regasification terminals, or the Otranto Channel for the Adriatic ones. The result is a significant operational asymmetry: the Otranto Canal, as the only maritime access route to the northern Adriatic, therefore unconditionally constrains, whatever the origin of the cargo, the entire Adriatic regasification capacity, while the criticality of the Strait of Sicily is a function of the supply mix and grows in proportion to the share of LNG arriving via Suez. The gradual replacement of the Qatari molecule with the US one, accelerated by the Red Sea and Hormuz crises, therefore mitigates the pressure on the Strait of Sicily as an outlet corridor for Suezini flows, but does not in any way loosen the constraint of the Otranto Channel on the Adriatic terminals.

This internal dependence is superimposed on an "upstream" dependence on *extra-Mediterranean choke points* on the same flows: a Qatari cargo bound for Porto Levante crosses the Strait of Hormuz, the Bab el-Mandeb, the Suez Canal, and the Otranto Canal in series with proximity also to the Strait of Sicily. Five consecutive bottlenecks. The first three are entirely outside national and European control; the last two, although close to the national territory, remain international navigation corridors whose legal regime limits the instruments of unilateral control of the coastal state. The fragility of this serial chain has been manifested in two recent episodes. The Red Sea crisis has effectively closed the Bab el-Mandeb to LNG traffic since the end of 2023, compressing LNG carrier transits via Suez from about 32 million tons in 2023 to about 4 million in 2024, with Qatari canal volumes plummeting to negligible levels and diverted around the Cape of Good Hope¹³. The 2026 Strait of Hormuz crisis, with the closure declared by Iranian forces in March, QatarEnergy's force majeure following the attacks on the Ras Laffan complex, a gradual reopening that began in June, temporarily took away a significant share of Qatar's supply, which covers 12-14% of LNG imported by the European Union, from the European market^{14 15}. The strategic fact for the Italian system is that each of these upstream interruptions redistributes flows between the terminals and, with them, the load on the two national channels: each move towards the Atlantic origin intensifies the transits through the Strait of Sicily for cargoes bound

¹² Adriatic LNG, *Adriatic LNG launches Open Season 2025*, press release, 1 September 2025, <https://www.adriaticlng.it/en/media/press-releases/corporate/open-season-2025-en>

¹³ Kpler, US-Houthi truce may spur LNG flows via Red Sea and Suez Canal; gradual recovery expected, May 8, 2025, <https://www.kpler.com/blog/us-houthi-truce-may-spur-lng-flows-via-red-sea-and-suez-canal-gradual-recovery-expected>

¹⁴ Congressional Research Service, *Iran Conflict and the Strait of Hormuz: Impacts on Oil, Gas, and Other Commodities*, R45281, Washington D.C., 2026, <https://www.congress.gov/crs-product/R45281>

¹⁵ Bloomberg, *Qatar plans quick LNG output recovery as Hormuz reopening nears*, June 16, 2026, <https://www.bloomberg.com/news/articles/2026-06-16/qatar-plans-to-rapidly-restart-lng-production-after-hormuz-opens>

for the Adriatic, making the Sicily-Otranto combination not a static constraint but a variable dependent on the changing geography of the offer.

In this context, the Otranto Canal deserves further qualification: it is at the same time an obligatory transit corridor for LNG carriers bound for the Adriatic terminals and the site of fixed infrastructure on the seabed, with the offshore section of the TAP that passes through it to land in Melendugno. In the same confined space, therefore, both dimensions of underwater energy dependence, the mobile flow and the installed asset, converge, making the canal the most accomplished case, in the national perimeter, of overlap between corridor vulnerability and infrastructure vulnerability.

As regards the construction and management of high- and extra-high-voltage submarine electricity transmission infrastructures, they are mainly the responsibility of Terna, as operator of the National Transmission Grid (NTG). In this case, Terna's portfolio of submarine assets includes some of the most technologically advanced infrastructures in the Mediterranean basin.

The most systemically important links are in the Tyrrhenian basin and include:

5. **SA. PE.I. (Sardinia-Peninsula Interconnection):** 500 kV HVDC connection with a capacity of 1,000 MW and a total development of approximately 435 km, of which more than 420 km are submarine sections. The cable reaches depths of the order of 1,600 metres, placing it among the deepest HVDC infrastructures in the world at the time of its construction, as well as the longest 1,000 MW submarine cable in the world.
6. **Sa.Co.I.3 (Sardinia-Corsica-Italy 3):** new infrastructure in HVDC technology intended to replace and enhance the existing connection, improving the energy exchange capacity between Sardinia, Corsica and Tuscany.
7. **Tyrrhenian Link:** an infrastructural scale leap project that provides for a double 500 kV HVDC connection divided into two branches - one between Sicily and Campania (east branch) and one between Sicily and Sardinia (west branch) - for a total development of about 970 km and a transmission capacity of 1,000 MW for each branch. Conceived as a strategic corridor in the central Mediterranean, it is aimed at increasing the exchange capacity between market macro-areas and facilitating the integration of renewable energy in the South

On the Adriatic side, the most important infrastructure is the Italy-Montenegro interconnection: an HVDC connection of about 445 km (of which over 420 km at sea) with a capacity of 600 MW, which allows bidirectional exchange between the Italian and Balkan grids. At the same time, the GRITA 2 project is being developed with the Greek operator IPTO (Independent Power Transmission Operator), which provides for a new submarine power line of up to 1,000 MW for a total length of about 300 km (of which about 240 km at sea), aimed at strengthening the integration of the electricity market in South-Eastern Europe. Also, regarding submarine electricity infrastructure, the Strait of Sicily remains relevant with the Italy-Tunisia interconnection (ELMED). ELMED, with an expected capacity of 600 MW and an estimated length of between 200 and 220 km, is developed by Terna in collaboration with STEG (*Société Tunisienne d'Electricité et du Gaz*) with the aim of directly connecting the European and North African electricity systems, promoting the integration of new renewable capacity and strengthening energy security in the central Mediterranean basin.

Finally, in addition to these infrastructures, there are those on the offshore wind generation front: Italy is in a phase of rapid project expansion that will have direct repercussions on the extension of the submarine power cable system. To date, 93 offshore wind farm projects distributed in the waters of ten coastal regions have been filed for aggregate power in the order of tens of gigawatts. Almost all the proposals (88 out of 93) concern floating technology plants, with an average distance from the coast of more than 30 kilometers. The regions with the highest number of initiatives are Puglia (26 projects), Sicily (25) and Sardinia (24), outlining a southern axis as the main area of development in the sector. The expected expansion of offshore wind will significantly increase Italy's surface area of exposure in the underwater dimension, adding new connection cables to the continental grid, new coastal logistics nodes and new systemic interdependencies between offshore production and the transmission grid.

1.4 Choke points and areas of greatest vulnerability

The joint analysis of the distribution of telecommunications infrastructures, the gas system and the submarine electricity grid reveals a geographical structure characterized by a strong spatial concentration, sectoral interdependence and connection to *choke points* of both regional and global importance. This configuration determines a risk profile that is not simply the sum of the risks of each infrastructure considered individually, but a systemic risk emerging from their overlapping in restricted geographical spaces. Overall, the map of landing points also confirms a dynamic of strong concentration. A significant share of telecommunications cable landing points, a significant part of transnational gas pipeline landings and power lines are concentrated in a few regions, configuring potential *acronyms of a territorial nature*.

The Strait of Sicily and the central Mediterranean constitute the area of greatest strategic sensitivity for Italy. In this corridor, the main communication and energy routes overlap in a particularly evident way: intercontinental internet backbones, gas pipelines from North Africa and new generation transnational power cables converge towards the same Sicilian landings in the same maritime space. Sicily is both a landing and transit point for internet backbones connecting Europe, the Middle East and Asia, and concentrates landings and energy infrastructures from the African continent. This convergence increases resilience only if accompanied by redundancy and restoration capacity: in the absence of these conditions, it transforms the territory into a risk multiplier, in which an accident or a hostile act in a geographically restricted area can generate cascading effects on both data traffic and energy flows. The Adriatic-Ionian quadrant, and particularly the Otranto Channel, is a second corridor of high strategic importance. The TAP pipeline, transnational power cables to Greece and the Balkans, and digital routes of increasing importance converge in this space. The geographical proximity to areas of instability in the eastern Mediterranean amplifies the strategic value of this corridor.

If we then extend the analysis beyond the national perimeter, a further vulnerability emerges *global choke points* condition the integrity of Italian infrastructures even though they are outside the sovereignty, jurisdiction or in any case geographical proximity of the State. The most obvious case is the Suez Canal, which constitutes a *global choke point* for data flows between Europe and Asia: The concentration of internet backbones that transit through this channel, and their exposure to regional

instability dynamics, makes Italy indirectly vulnerable to events that occur thousands of kilometers from its coasts.¹⁶

The most relevant risk profile is not exclusively that of the deliberate attack. The systemic fragility produced by accidental accidents, natural events and the domino effect between damage to energy and digital networks represents an equally concrete threat whose management requires an integrated approach that the following sections aim to analyze and develop starting from the regulatory context for the construction, management and protection of infrastructures, and then analyze specific risks and possible defense solutions.

¹⁶ As explained in the following paragraphs, surface kinetic actions not directly aimed at underwater pipelines, such as attacks on merchant ships or repair ships, can also have repercussions on the resilience of infrastructure on the seabed.

8. Regulatory and jurisdictional perimeter of the underwater dimension

Among the main legal issues concerning critical submarine infrastructures, two are the subject of increasing attention: the scope of the actors' competences and their liability. As regards the scope of competence, the debate focuses on the effective room for manoeuvre of the armed forces for monitoring, surveillance, prevention and intervention in the event of criminal actions against infrastructures that have occurred in international maritime spaces. Regarding the issue of liability, it is controversial both whether the companies that own the infrastructures that provide public good are responsible for the damage suffered by the company, and whether the armed forces are responsible for the functionality of the companies. In both cases, there is a discussion of omission, negligence and readiness in restoring the public service and possible compensation for the damage suffered and costs incurred by the company.

2.1 The sovereignty and jurisdiction of the coastal state

The United Nations Convention on the Law of the Sea of 10 December 1982 (UNCLOS)¹⁷ is the main instrument for codifying the Law of the Sea and clearly identifies the prerogatives of the coastal State in the maritime spaces off the coast.

In territorial waters, the coastal State exercises, in particular, full sovereignty over the seabed, soil and subsoil below, being able to regulate the laying and protection of cables, pipelines and infrastructures by means of laws and regulations, including within the framework of the regulation of innocent passage (Art. 21 UNCLOS). The coastal State may protect cables and pipelines, it being understood that its laws may not concern the design, construction, rigging and fitting out of foreign ships unless they implement generally accepted international standards or regulations (e.g. the regulations of the International Maritime Organisation).

In the contiguous area, the UNCLOS grants the coastal State *preventive* or repressive enforcement powers in the event of violations of laws and regulations on customs, taxation, health and immigration committed on land, in internal waters and in the territorial sea (Article 33). A generic regime of freedom of navigation is in force, including submerged. Other States are also granted the freedom to lay submarine pipelines and cables, in compliance with the regime of the continental shelf or the Exclusive Economic Zone (EEZ) that may be applicable beyond the external limits of the territorial sea. By Law No. 70 of 7 May 2026, Italy has started the process of proclaiming the contiguous zone with the consequent updating of the baselines.

In the EEZ, UNCLOS balances the sovereign rights of the coastal state in relation to the exploration, exploitation and conservation of resources and the freedom of other states to lay cables and pipelines. Sovereign rights include coercive powers (Art. 73 UNCLOS) and competing with the courts in the context of economic activities relating to water, the seabed, soil and subsoil (Art. 56 UNCLOS). In this area, the coastal state can establish reasonably sized "safe zones" around infrastructure (Art. 60 UNCLOS), which has the potential to protect critical underwater infrastructure.

¹⁷ United Nations Convention on the Law of the Sea, Montego Bay, 10 December 1982, UNTS 1833. In force since 16 November 1994.

As regards the continental shelf, Art. 79 UNCLOS recognises the right of all States to lay cables and pipelines but gives the coastal State the right to adopt measures and establish conditions when the infrastructure is related to the exploitation of its resources, its territorial sea or its territory. All States must consider the infrastructure already in place, in order not to jeopardise its repair.

Open point: The definition and practical implementation of the "safety zones" pursuant to art. 60 UNCLOS around critical Italian submarine infrastructures in the EEZ require specific operational and regulatory elaboration, in coordination with the Agency for the Safety of Underwater Activities (ASAS). The absence of formally delimited perimeters reduces the capacity for deterrence and preventive enforcement.

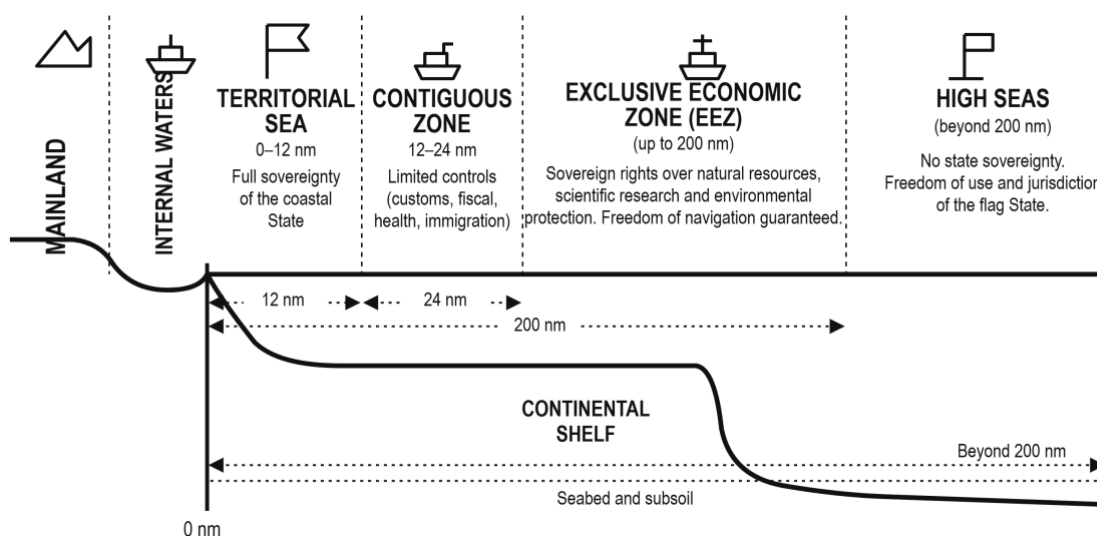


Figure 5. Distribution of maritime spaces according to UNCLOS¹⁸

2.2 The grey areas of the high seas: limits of enforcement mechanisms and regulatory gaps

It is on the high seas and on the seabed beyond the continental shelf that the regulatory framework reveals its most critical shortcomings. Art. 87 UNCLOS includes the laying of cables and pipelines among the freedoms of States, while art. 112 establishes the right to lay them beyond the continental shelf. However, protection mechanisms and enforcement powers remain seriously insufficient in the face of contemporary threats.

Art. 113 UNCLOS obliges States to criminalize in their legal systems the intentional or negligent breakage or damage to cables and pipelines on the high seas by flag ships or persons under their jurisdiction. Arts. 114 and 115 respectively provide for liability for damage caused to other people's infrastructures during laying operations and the obligation to compensate ship owners who have sacrificed equipment to avoid damage to cables. This body of legislation, however, has not been uniformly implemented by States and is based entirely on the cooperation of the flag State and its willingness to activate its criminal jurisdiction, an assumption that often proves to be illusory.

¹⁸ Authors' elaboration on CNUDM

Moreover, the mechanism of exclusive jurisdiction of the flag State creates a structural vulnerability in the case of ships belonging to "shadow fleets" or flags of convenience operating on the high seas damaging infrastructure. In such cases, there is no effective control by the flag State, and the damaged coastal State does not have, from the point of view of these provisions, any autonomous legal title to intervene, stop or seize such vessels.

The Paris Convention of 14 March 1884 on the protection of submarine telegraph cables, the application of which is safeguarded by art. 311 UNCLOS, is still in force in relations between the 36 Contracting States, including Italy and the United States, and assigns criminal jurisdiction to the courts of the flag State for crimes committed on board ships (art. VIII). Although the convention may cover electric cables, fiber optic cables and telephone cables, it remains inadequate on several fronts: it does not cover crimes not committed on board, it is ineffective in the presence of ships without flags or flying flags of convenience and does not provide for powers of visit and inspection without the consent of the flag State.

The right of inspection and inspection granted to warships on the high seas is in fact limited to ascertaining the nationality of the ship and obtaining evidence on the disputed facts (art. 10 of the 1884 Convention). In any case, boarding for seizure or hijacking remains subject to the consent of the flag State. The right of visit referred to in art. 110 UNCLOS is broader but concerns exhaustively listed cases in which damage to a cable or submarine infrastructure does not fall.

Some commentators have proposed that attacks on cables and conducts should be classified as piracy (Articles 100-106 UNCLOS), thereby justifying the right of access pursuant to Art. 110 and universal jurisdiction pursuant to Art. 105, but this interpretation is not convincing: piracy requires the pursuit of private ends, while the most dangerous attacks on underwater infrastructures are generally motivated by political, strategic or hybrid reasons.

The right of pursuit pursuant to Article 111 of the UNCLOS allows the coastal State to extend jurisdiction on the high seas over foreign ships that have committed offences in the waters subject to its sovereignty. This instrument is applicable where the damage to an infrastructure originates or has effects in the territorial waters or in the Italian EEZ in violation of Italian laws, and constitutes a relevant operational lever for the Navy, to be activated promptly before the foreign ship reaches the territorial waters of another State.

The figure of the "navigation accident" pursuant to Article 97 UNCLOS could cover damage to "*submarine telegraph, telephone or high-voltage power cable or to a pipeline*" according to the *United Nations International Law Commission*. The provision justifies the exercise of criminal jurisdiction by both the flag State and the State of nationality of the master or crew member responsible. However, only the flag State retains the power to stop and seize the ship (Article 97, par. 3). It follows that, even in the presence of an accident involving an Italian infrastructure on the high seas, the Navy cannot proceed with the arrest of the ship without the consent of the flag State.

In this scenario, when the accident at sea generates pollution, art. 221 UNCLOS allows coastal States to adopt, beyond the territorial sea, measures proportionate to the damage suffered or foreseeable, to protect their coasts from pollution or a threat of pollution. Although it does not explicitly refer to damage to infrastructure, the rule can

be invoked extensively to legitimize emergency interventions even on the high seas, if there is a risk of contamination or environmental damage related to the damage to pipelines.

2.3 Other relevant international instruments and liability profiles

In addition to UNCLOS, some international instruments may justify the exercise of criminal jurisdiction based on the territorial connection of the effects of the crime, the nationality of the perpetrator or victim, or the principle of protection of interests common to several States. The United Nations Convention of 15 December 2000 against transnational organized crime (Palermo Convention)¹⁹ offers a framework in this regard applicable when damage to infrastructures assumes the characteristics of organized and cross-border crime falling within the scope of the Convention.

The Rome Convention of 10 March 1988 for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,²⁰ on the other hand, has limits of application with respect to underwater infrastructures on the high seas: although it covers crimes against navigation, including those involving submarines, which can potentially be configured as predicate crimes for damage to infrastructures, it does not easily extend to harmful conduct carried out directly against cables or pipelines.

In terms of international investment, several bilateral treaties (BITs) include maritime areas in the notion of "territory" and can classify underwater infrastructure as "foreign direct investment". The "*full protection and security*" clause provided for by many BITs imposes positive physical protection obligations on the host state, with potential implications for the international liability of the coastal state in the event of damage to foreign-owned infrastructure operating in its maritime space.

Open point: The legal basis of the jurisdiction of the State of nationality of the owner of the underwater infrastructure on the high seas remains uncertain and uncoded. The absence of a clear conventional title exposes the interventions of the Navy to disputes of legality at international level, requiring a case-by-case assessment of the existence of alternative legal bases, also in combination with bilateral or multilateral cooperation agreements.

2.4 The Italian regulatory framework: Law 9/2026 and the new competences of the Navy

At the national level, Law No. 9 of 26 January 2026 (Law 9/2026)²¹ significantly reformed the Code of Military Order (COM), introducing provisions expressly dedicated to the protection of underwater infrastructures of national interest. The definition of such infrastructures, contained in art. 2, par. 1, letter n), covers, under certain conditions, both installations located in Italian maritime spaces and those located on

¹⁹ United Nations Convention against Transnational Organized Crime (Palermo Convention), 15 December 2000, UNTS 2225.

²⁰ Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Rome, 10 March 1988, UNTS 1678.

²¹ Law no. 9 of 26 January 2026, containing provisions on the safety of underwater activities and amendment of the Code of Military Order (Legislative Decree no. 66 of 15 March 2010).

the high seas, reflecting the operational reality of an infrastructure network that extends well beyond territorial waters.

In terms of the prerogatives of the Navy, the reform is divided into several levels. Art. 111, paragraph 1, letter d-ter COM, now contemplates the protection of the national underwater infrastructure by force in the event of destruction, damage or tampering, in compliance with applicable international law. Art. 111, paragraph 1, letter d-quarter gives the Navy control over inland waters, the territorial sea and the continental shelf for military defense purposes, expressly including the prevention of unauthorized underwater navigation. Art. 111, paragraph 1, letter d-quinquies establishes the competence to cooperate with the navies of allied or neighboring states for the surveillance of underwater infrastructures.

The same Law 9/2026 established the ASAS, called upon to carry out functions of coordination, international representation and development of policies for the protection of underwater infrastructures, even in spaces without sovereignty and jurisdiction. The ASAS is required to operate in close connection with the Navy, as well as with the National Cybersecurity Agency (ACN) in view of the dual nature (physical and digital) threats to underwater infrastructure. A similar connection should exist with the EU Agency for Cybersecurity (ENISA) beyond the dictates of Law 9/2026.

The central issue remains that of liability. While critical submarine infrastructures are subject to the EU *compliance regime*, the military sector intervenes in the management of related crises from a national security perspective. In the event of omissions or negligence in the exercise of surveillance and protection activities, the responsibility is borne by the State, because of the conduct of its armed forces. On the other hand, the Navy can operate as a contracting authority if it makes use of private individuals to better organize the surveillance and protection functions. In this case, the responsibility is borne by the entity in charge of the surveillance and protection tasks, but recourse actions are possible where the damage derives from malfunctions of the service contracted to the private player.

The Navy carries out surveillance activities, offers technical and operational support and intervenes in emergency situations. It should be remembered that Law 9/2026 assigns these functions to it in connection with the broad concept of "underwater infrastructures of national interest". The memoranda of understanding between the Navy and critical entities distributes the tasks of surveillance and assistance, so that the technology developed by the latter serves the security functions carried out by the former. In principle, these protocols do not alter the framework of the owners' responsibilities and responsibilities. The critical entity retains ownership or co-ownership of the cable, which entails responsibility for the maintenance and continuity of the technical service. The Navy assumes functions and responsibilities in the field of safety and protection from external agents. The two responsibilities are placed on different levels if the activity is carried out in accordance with the memoranda of understanding or other agreement.

Law 9/2026 makes it clear that the Navy's competence extends well beyond the spatial limits of Italian sovereignty in the case of "underwater infrastructures of national interest" located on the high seas, landing or departing from Italian territory. Consequently, forms of negligence or inexperience that cause or contribute to causing the occurrence of an "accident" on the high seas are attributable to the Navy in general, if stationed to oversee the infrastructure of national interest and, in the CER framework

in particular, if the effects of the accident also (or only) materialize in Italian territory. Similarly, the responsibilities of the critical party extend to the entire structure, for the part of the competence of the subject itself, possibly defined based on agreements with foreign partners. Any fact that affects the resilience of the cable in Italian territory generates liability regardless of where it happened (e.g. on the high seas) if, with respect to the fact (e.g. maintenance defect) such liability is attributable to the critical party.

Open point: The European directives NIS 2²² and CER²³ do not apply to the sectors of the administration that carry out their activities in the sectors of national security, public security or defence (art. 1, par. 6 CER; art. 2, par. 7 NIS2). However, private critical entities that own or co-own cables and infrastructures are subject to it. The Navy is called upon to interact with these entities through memoranda of understanding that clearly allocate responsibilities: critical entities retain responsibility for the maintenance and continuity of the service; the Navy assumes the functions of security and protection from external threats. Recommendation (EU) 2024/779²⁴ and the EU Action Plan on Cable Security orient towards a holistic and integrated approach, to which the Navy is called upon to actively contribute.

2.5 Ideas for cooperation and strategic projection

International cooperation is the essential tool to fill the regulatory gaps that characterize the dimension of the high seas. In the absence of coercive multilateral mechanisms, the most effective way in the short to medium term is that of operational cooperation and *soft law*: the development of shared principles, collections of good practices, bilateral and multilateral agreements for joint surveillance and exchange of information.

A relevant example, albeit of regional scope, is represented by the coordination initiatives launched within NATO for the protection of critical underwater infrastructures in the North Atlantic theater²⁵, in response to the episodes of damage to the Nord Stream pipelines in September 2022, the attribution of which remains controversial. These episodes have shown that the vulnerability of underwater infrastructure is not theoretical, and that the legal and operational response tools available proved insufficient in the immediate aftermath of the incident. A more recent framework of operational cooperation has been outlined in the *Guiding Principles for Underwater Infrastructure Defence Exchanges (GUIDE)*.²⁶

The Navy is now expressly authorized by the COM, as amended by Law 9/2026, to promote and participate in forms of cooperation with the navies of allied or neighboring states for the surveillance of underwater infrastructures. This competence should be

²² Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS 2) on measures for a high common level of cybersecurity across the Union, OJ L 333, 27.12.2022.

²³ Directive (EU) 2022/2557 of the European Parliament and of the Council (ERC) on the resilience of critical entities, OJ L 333, 27.12.2022.

²⁴ Recommendation (EU) 2024/779 of 26 February 2024 of the European Commission on the safety of submarine cables, OJ L, 8 March 2024.

²⁵ NATO, "NATO steps up its support to protect critical undersea infrastructure," press release, 2022. Available on: <https://www.nato.int>

²⁶ Launched in May 2026 on the sidelines of the 23rd Shangri-La Dialogue in Singapore, the initiative involves 17 states (including Italy) and aims to implement a framework for international defence cooperation to support the security of critical underwater infrastructures.

translated into technical-operational agreements that provide for coordinated surveillance, intelligence sharing, rapid response protocols and the definition of shared responsibilities — even in areas beyond national jurisdiction. Together with ASAS, the Navy can be a candidate to play a leading role in defining common standards at the Euro-Atlantic level, helping to reduce the regulatory fragmentation that today favors the impunity of hostile actors.

Open point: The classification of underwater infrastructure as military targets in an armed conflict is permitted by the law of armed conflict when such infrastructure is functional to the operations of enemy armed forces or their war effort. The Fourth and Fifth Hague Conventions govern the conditions of lawfulness, including the principle of "absolute necessity", respect for neutral waters and the prohibition of destroying cables connected to a neutral State. The Navy must integrate these constraints into its operational doctrine, especially in crisis scenarios of varying intensity.

9. Risks and threats to subsea infrastructure

Today's threats are reduced compared to potential future threats due to at least three fundamental elements: 1) the proliferation of low-cost weapons such as marine drones, 2) the increase in international tensions; 3) the preparation of future threats (mapping of infrastructures, pre-positioning of latent tools, etc.) that could have a significant impact in the event of future conflicts.

3.1 Scope of analysis

One of the most important conceptual acquisitions of risk analysis in the underwater dimension is the overcoming of the reductionist vision that considers the infrastructure exclusively as a physical object understood as a cable, a pipe, a steel pipe lying on the seabed. Underwater infrastructures are complex systems, divided into physical, digital and organizational components that interact along a life cycle extended in time and distributed in space. It follows that the safety of the infrastructure is not reducible to the protection of the submerged section (*wet plant*) but depends on the operational reliability of the entire system²⁷.

This principle has direct operational implications. A physically intact infrastructure can be compromised by an attack on its digital management system; a fully functional cable can become unusable if the landing station that connects it to the terrestrial grid is down. A perfectly intact pipeline can be rendered inoperable if the maintenance vessel that is supposed to intervene in the event of a failure fails to access the territorial waters of the relevant coastal state. In this context, any analysis that is limited to the submerged component alone would miss the substance of the problem.

It follows that the submarine infrastructure must be treated as a distributed socio-technical system and not as a simple linear artifact laid on the seabed. In fact, vulnerability does not coincide with the physical exposure of the cable or pipeline alone, but with the combination of: (i) concentration of land and logistics nodes; (ii) industrial and supply chain dependencies; (iii) information and digital dependencies; (iv) intervention and repair capabilities; (v) regulatory and authorization frameworks that condition response and recovery times. The attack and failure surface is therefore distributed along a chain of heterogeneous assets, actors and processes. This has direct implications for the setting up of any protection and surveillance plan.

3.1.1 The five levels of the infrastructure system

For analytical purposes, the life cycle of a diving infrastructure is divided into five distinct phases, each with specific vulnerabilities.

The extension of this life cycle and the different risk exposures that the infrastructure has at each stage determine the need for a defense approach with a broad view of the problem and threats, such as not to neglect possible blind spots or the defense of a specific aspect.

²⁷ European Commission Expert Group, Report on the Security and Resilience of EU Submarine Cable Infrastructures, 2025.

Governance and planning: The first level concerns the actors and dynamics that influence the ownership structure and the route of the infrastructure. Pipelines are predominantly owned by energy companies interested in connecting their offshore fields to outlet markets; communication cables belong to big tech or consortia of telecommunications companies; power cables mostly belong to transmission system operators (TSOs).

The initiative tends to be mainly private, although the role of the State can take on significant weight in the presence of companies with public participation or operating in strategic sectors. The route of the infrastructures is influenced by commercial needs, the morphology of the seabed, maritime traffic and environmental impacts on the marine ecosystem²⁸.

Construction and supply chain. The second level concerns the construction, assembly and supply chain of the infrastructure. The main players are a few highly specialized companies (suppliers) to which the owners entrust the construction. The market concentration among a small number of manufacturers (Alcatel Submarine Networks, Subcom, NEC Corporation and Elettra TLC) creates structural dependencies that are difficult to reverse in the short term²⁹.

Installation. The third level concerns the laying of the infrastructure on the seabed, entrusted to highly specialized ships. In the case of communication and electrical cables, the installation is carried out by a limited number of cable-laying vessels equipped with dynamic positioning systems; for energy pipelines, *Construction Service Vessels* (CSV) designed for complex welding and laying operations are used. During installation, both types of infrastructure can be buried to increase protection by means of marine ploughs or ROVs up to a depth of about 1,000–1,500 m. Bathymetry affects the diameter of the cable: in the first few meters the pipeline is thicker, decreasing in thickness as the depth increases.

Operation. The fourth level concerns the ordinary management of the infrastructure after installation. For communication cables, commissioning includes *end-to-end* testing, configuration of *terminal equipment* and activation of OSS/NMS monitoring systems for the detection of faults, degradations and anomalies. Commercial capacities (IRU, leasing) are also allocated, and protection and recovery mechanisms are configured (*rerouting*, *automatic switching*, alarm thresholds).

For HVDC power cables, commissioning requires insulation testing, testing of converter stations, and integration with the grid operator's operating functions. For offshore pipelines, the phase includes *pre-commissioning*, controlled flow start-up, and calibration of SCADA systems.

Repair and maintenance. The fifth level concerns the response to failures and damages. Repair is the responsibility of the owner companies but is entrusted to private parties with specialized vessels, often different from those used for installation. For electrical cables and pipelines, TSOs enter into multi-year framework agreements with specific repair companies. For communication cables, there are club agreements (with sharing of resources between several owners) and *private maintenance* agreements (with

²⁸ European Maritime Spatial Planning, Cables and pipelines & Marine protection and restoration.
²⁹ Submarine Telecoms Forum (2026), Industry Report 2025-2026.

direct control of the owner). The global average time between fault detection and restoration is about forty days, a strategically relevant exposure window.

Modern cable systems are all designed with automatic recovery capabilities via network management software.

3.2 Undeliberate threats

A comprehensive analysis of threats to underwater infrastructure requires first to distinguish the intentionality of the action. Damage to seabed pipelines often occurs for reasons unrelated to intentional human actions. Therefore, it is necessary to adequately consider the framework of unintentional threats, which represent the main cause of damage to underwater infrastructure globally³⁰.

3.2.1 Natural threats

Risks from natural phenomena pose a significant threat to the resilience of underwater infrastructure, although they are often underestimated in conventional safety analysis. A recent study led by the UK's National Oceanography Centre (NOC) found that around 25% of damage to submarine communication cables between 1965 and 2019 was attributable to natural causes.³¹

Extreme events such as typhoons, underwater landslides, currents, and volcanic eruptions can cause widespread damage to multiple systems at once. The January 2022 eruption of the Hunga volcano in Tonga destroyed the archipelago's only international cable, isolating the country for weeks and severely hampering emergency response. In the Gulf of Guinea, between January and March 2020, turbidity currents in the Congo Canyon repeatedly damaged cables, disrupting internet services across West Africa.

Lower intensity phenomena, such as continuous storms and persistent sea currents, can also contribute significantly to failures: a new analysis of historical cases reveals that a significant percentage of previously unattributed damage could be related to such low intensity but prolonged impacts over time.³²

Climate change is also a long-term multiplier, as it could increase both the magnitude and frequency of these phenomena, with significant repercussions also on pipelines, which are particularly exposed to hydrodynamic repercussions due to currents.³³

³⁰ Kordahi, M. E. et al. (2019), "Global Trends in Submarine Cable System Faults 2019 Update", *Proceedings of the SubOptic 2019*, New Orleans, USA; Clare, M. (2021), *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), Issue 2

³¹ Bricheno, L. et al. (2024), "The diversity, frequency and severity of natural hazard impacts on subsea telecommunications networks", *Earth-Science Reviews*, Vol. 259, 104972 <https://doi.org/10.1016/j.earscirev.2024.104972>

³² Clare M., et al. (2023), "Climate change hotspots and implications for the global subsea telecommunications network," *Earth-Science Reviews*, Vol. 237, 104296, <https://doi.org/10.1016/j.earscirev.2022.104296>.

³³ Durap, A. & Can, E. B. (2022), "Risk assessment of submarine pipelines: A case study in Turkey", *Ocean Engineering*, Vol. 261, 112079, <https://doi.org/10.1016/j.oceaneng.2022.112079>

Human action has little capacity to act on the causes of these threats; however, it remains possible to adjust management and defense actions to limit adverse effects.

3.2.2 Accidental anthropogenic threats

Damage resulting from purely natural causes constitutes only a small part of the failures of underwater infrastructure. In most cases, damage is caused by accidental human activities. Dragging of anchors and fishing nets is by far the leading cause of damage to submarine cables, with estimates ranging from 60% to 86% depending on the sample analyzed³⁴.

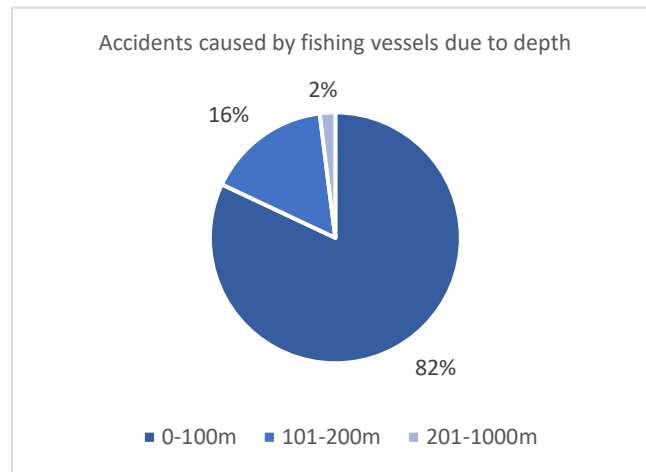


Fig. 2 — Main categories of submarine cable failure by cause

Trawling. Trawl (divergent) doors and weights designed to lift marine sediment pose a real threat. In 90% of cases, contact between nets and cables does not cause damage, but the use of grappling hooks to retrieve nets significantly increases the risk of hooking, especially in the case of infrastructures that are not sanded and without reinforcement.³⁵ In this sense, the progressive increase in fishing depth, induced by the depletion of fish stocks and climate change, constitutes a danger because at higher bathymetric times the pipelines are neither silted nor reinforced.

Anchor dragging. Since 2011, thanks to ICPC studies, it has been shown that anchors represent a much more significant cause of damage than previously thought. The dangers are particularly significant in waters below 200 m, where almost all this type of damage occurs.³⁶ Damage can occur both when an anchor is lowered directly onto a cable and when it is unintentionally dragged over long distances.

³⁴ Kordahi, M. E. et al. (2019), "Global Trends in Submarine Cable System Faults 2019 Update", *Proceedings of the SubOptic 2019*, New Orleans, USA,; Clare, M. (2021), *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), Issue 2,

³⁵ Clare, M. (2021), *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), Issue 2, https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf

³⁶ International Cable Protection Committee (2025), *Damage to Submarine Cables from Dragged Anchors*, <https://www.iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/>

In the Baltic Sea, since 2022, merchant ship anchors have caused damage to more than ten underwater infrastructures, including the Balticconnector gas pipeline between Finland and Estonia. All these cases have suspicious characteristics that place them in a gray area between accidental damage and deliberate sabotage: in fact, the crew has almost always stated that they did not notice the anchor at sea, dragged for long stretches hitting several nearby infrastructures.

The problem is amplified by the fact that many commercial shipping lanes transit through the same geographical areas where subsea infrastructure is concentrated, and that cable location maps are not always fully accessible or up to date for all seafarers.

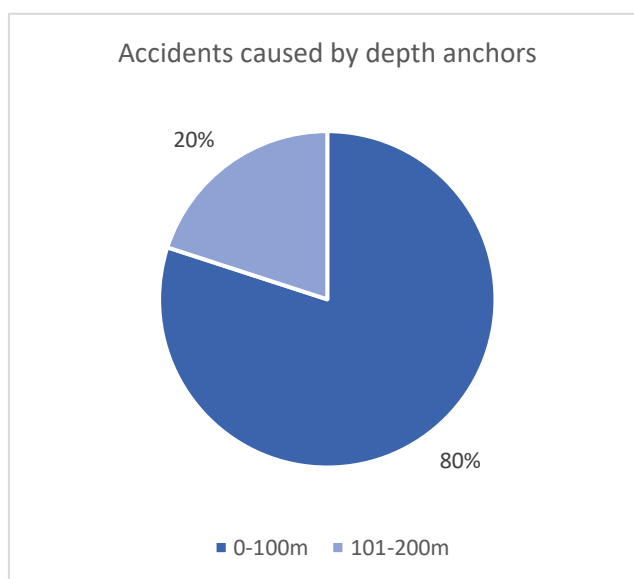


Fig. 3 — Anchor damage mode on submarine cable.

Conflicts and war zones as an indirect risk. Kinetic actions on the surface can affect underwater infrastructure indirectly. In February 2024, the crew of the merchant ship Rubymar (hit by a Houthi ballistic missile) dropped anchor before abandoning ship, and the drifting vessel damaged four communication cables laid on the bottom of the Red Sea.

The presence of active conflicts also makes normal installation and repair operations impossible, as cable-laying vessels operate at extremely low speeds and must remain stationary during repairs. The cost of securing cable-laying vessels near Yemen has increased to \$150,000 per day, hampering the commissioning of Blue-Raman and 2Africa cables, affecting route redundancy and connectivity on the African continent.³⁷

3.3 Deliberate and hybrid threats

Threats arising from deliberate anthropogenic actions are characterized as hybrid threats, with actions that combine conventional and unconventional, physical and

³⁷ Leccese, G. (2025), "Choke point Above and Below the Surface: The Red Sea's Emerging Infrastructure Challenge", *Istituto Affari Internazionali (IAI)*, Brief, no. 8, <https://www.iai.it/it/pubblicazioni/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge>

digital, state and quasi-state means, to produce effects that deliberately remain below the conventional response threshold.³⁸

The essential characteristic of the hybrid threat is the deliberate ambiguity with respect to the identity of the actor, the underlying intentions and the nature, hostile or accidental, of the event. This ambiguity delays or prevents an immediate response, since the victim must gather evidence of imputability before a coercive measure can be justified, and erodes trust in the availability and reliability of infrastructure in the long run.

In fact, the operational logic favors the production of decision-making uncertainty and the artificial extension of recovery times (the global average of about forty days between fault detection and recovery represents a window of strategic exploitability), rather than the destruction of the asset.

This logic is favored by three structural factors: (i) the plurality of actors, with deliberately blurred lines of demarcation between state actors, criminals, proxies and private operators; (ii) legal-spatial fragmentation, with a regulatory mosaic that makes it difficult to attribute hostile acts; (iii) the dependence on limited capacities (repair ships, specialized components, EMS/NMS software) whose availability can be conditioned as an act of hybrid pressure.

3.3.1 State actors

For over a century, hostile acts against underwater infrastructure have been carried out solely by state actors. The first known case dates back to 1898, during the Spanish-American War, when the United States cut several telegraph cables in the Philippines and the Caribbean to disrupt Spanish communications.

During World War I the first British move was the cutting of German telegraph cables; in World War II, Operation Saber saw the Allies cut two Japanese cables off Saigon to force the enemy to use interceptable wireless communications. During the Cold War, Operation Ivy Bells (1971) led to the installation of an induction pod by the U.S. specialized submarine USS Halibut to read Soviet cable messages in the Sea of Okhotsk.

Such hostile acts towards underwater infrastructure also characterize the new millennium, as evidenced by the operation, which emerged in 2013, with which the GCHQ (Government Communications Headquarters) of the United Kingdom connected to the network of Internet cables to access huge amounts of communications of innocents and suspects and then transmitted the information to the US *National Security Agency* (NSA). Today, state actors possess different capabilities to interfere with cables and pipelines on the seabed.

Russia has developed several specialized platforms for seabed operations. The oceanographic vessel Yantar, formally a scientific research vessel, is documented for close surveillance of NATO underwater infrastructure in the Atlantic and

³⁸ European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), *Protecting Maritime Infrastructure from Hybrid Threats: Legal Options*, Hybrid CoE Research Report 14 (Helsinki: Hybrid CoE, 2025), pp. 8–12. For the operational definition of "grey zone" in the maritime context, see. NATO, "Countering Hybrid Threats," NATO, updated on 29 January 2026.

Mediterranean, with capabilities to deploy mini-submarines and underwater drones, both remotely operated vehicle (ROV) and autonomous (AUV). The Russian arsenal also includes nuclear-powered submarines, such as the *Paltus*, the *X-Ray*, the *Kashalot* and the *Losharik*, specially modified to interact with the seabed at great depths through mechanical arms.³⁹

China, on the other hand, acts in the underwater dimension mainly through complementary vectors that make its threat profile multidimensional. On the cyber and intelligence level, it could compromise management systems (pre-positioning, access to the management plane) and exploit the supply chain. On the physical level, the vector observed is damage in shallow waters by merchant ships and "shadow fleets" (Taiwan 2025 cases), which seems to be accompanied by an emerging deep-sea capability with a strong signaling value as shown by the cable cutting device up to 4,000 meters revealed in 2025 and tested at 3,500 meters in 2026, which can be integrated with the Fendouzhe and Haidou submarines⁴⁰. On an industrial and geoeconomic level, the projection takes place through the Digital Silk Road and the presence of operators such as HMN Technologies (formerly Huawei Marine Networks) in tenders for new backbones, with the consequent issues of physical access to systems and potential compromise of components under construction and repair.

The United States boasts several possible attack vectors against underwater infrastructure. On the physical level, the US Navy in recent decades has used the specialized submarine USS *Halibut* for specific operations of interaction with the seabed and currently seems to have similar platforms with the nuclear submarine USS *Jimmy Carter*. The espionage programs revealed by Snowden, in particular TEMPORA and MUSCOLAR, conducted in collaboration with the British GCHQ, have documented the ability to intercept data carried by submarine cables both in the Atlantic and in the Pacific. The *Defend Forwards* (Cyber Command) doctrine provides for the deployment of offensive capabilities in adversarial infrastructures for deterrence and rapid response purposes. To these capabilities, there is the potential advantage given by the privileged position in the telecommunications cable sector of US hyperscalers, such as Meta, Google, Amazon and Microsoft, which could be involved in espionage operations as already happened in the case of PRISM.⁴¹

Iran represents a player of growing importance, both for the cyber capabilities developed by the APT (Advanced Persistent Threat) groups called APT33, APT34 and APT35 (also known as *Elfin*, *OilRig*, *Charming Kitten*), oriented towards intelligence collection and the disruption of industrial systems, and for the geographical control over the Strait of Hormuz, a global checkpoint for liquefied gas trafficking but a

³⁹ Kaushal, S. (2023), "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure", *Royal United Services Institute (RUSI)*.

⁴⁰ Silver, S. (2026), "China Just Proved It Can Cut Undersea Cables at 3,500 Meters Deep. Guam's 12 Fiber-Optic Lines Serve Google, the U.S. Military and the Entire Second Island Chain," 19FortyFive, April 19, 2026. <https://www.19fortyfive.com/2026/04/china-just-proved-it-can-cut-undersea-cables-at-3500-meters-deep-guams-12-fiber-optic-lines-serve-google-the-u-s-military-and-the-entire-second-island-chain/>

⁴¹ Snowden's revelations in 2013 highlighted how the US NSA, thanks to the PRISM program, had obtained the provision of data (e.g. emails, files, access notifications, etc.) from the main US technology companies that manage information, communications and user data in digital format (Microsoft, Facebook and Google), also spying on EU citizens and institutions. Cosmi, S. (2014), "NSA: "Google, Microsoft and Yahoo! knew everything about Prism": the head of the legal department accuses the web giants", *La Repubblica*, https://www.repubblica.it/tecnologia/2014/03/20/news/nsa_google_microsoft_e_yahoo_sapeva_no_tutto_di_prism_il_capo_dellufficio_legale_accusa_i_giganti_del_web-81428778/

potential point of vulnerability for the telecommunication cables laid on those seabeds. These infrastructures could be indirectly damaged during military operations on the surface, especially considering the Iranian use of naval mines.

A distinct category is that of actors whose relevance to the underwater dimension is indirect but not negligible, as it is based on the transferability of capabilities and proximity of interest. Although lacking documented underwater capabilities, North Korea has developed one of the most industrialized cyber offensive postures at the state level, oriented towards the generation of resources under *sanctions evasion* through the targeting of the traditional financial system (Bangladesh Bank/SWIFT case, 2016⁴²) and the theft of cryptocurrencies on a billion-dollar scale⁴³. What makes it relevant is not the predatory purpose itself, but the *modus operandi* that supports it, based on the compromise of digital supply chains and persistent access to critical systems, potentially oriented towards the telecommunications sector and submarine backbones if Pyongyang's strategic incentives change. Israel responds to the same logic for a different carrier: the consolidated tradition of precision cyber operations against industrial and control systems (Stuxnet as a paradigmatic case⁴⁴) expresses an OT/ICS capability that can be directly transferred to the SCADA systems of submarine pipelines and converter stations, to which is added a specific geographical interest for the infrastructures of the Eastern Mediterranean, the theater of data and energy backbones of increasing sensitivity such as EastMed. Finally, there is a growing number of medium-capacity state actors who are investing in the underwater dimension as a low-cost strategic asymmetry compared to conventional naval capabilities: for them, the barrier to entry is no longer the availability of sophisticated naval assets, but access to commercial unmanned technologies (ROVs/AUVs) and cyber market skills, with a threat profile destined to spread in a similar way to what has been observed for remotely piloted aircraft systems.

3.3.2 Non-state actors

Since 2007, the trend to interfere with underwater infrastructure, for years limited to state actors, has extended to non-state actors. Vietnamese fishermen have cut more than 500 km of submarine cables to extract materials for resale, causing the loss of more than 80% of Vietnam's connectivity. In 2015, suspicious cuts to cables near the California coast prompted the FBI to investigate possible acts of terrorism. In 2016, Somali pirates attacked a cable-laying ship during installation operations in the Red Sea.

In the cyber domain, the non-state threat converges on the system functions that make the infrastructure manageable and recoverable. It is therefore useful to distinguish four main profiles:

⁴² United States Department of Justice. (2018). Criminal complaint: United States v. Park Jin Hyok (Case No. MJ18-1479). U.S. District Court, Central District of California. <https://www.justice.gov/opa/press-release/file/1092091/download> ; See also: BAE Systems Applied Intelligence. (2016). *Two bytes to \$951m*. BAE Systems Threat Research Blog. <https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html>

⁴³ Chainalysis. (2025). 2025 crypto crime report: Stolen funds. Chainalysis.

⁴⁴ Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), ch. 15–1.

Hacktivists⁴⁵. Groups motivated by political or ideological reasons, with varying technical capabilities but generally inferior to those of state groups. They tend to demonstrative actions rather than operations with profound systemic effects but can cause significant temporary disruptions on management systems accessible via the internet⁴⁶.

Organized cybercrime. Transnational criminal organizations with increasing technical sophistication, motivated primarily by economic profit. They can pose a threat to cable operators' billing and operational management systems, as well as digital supply chains⁴⁷.

Insiders and contractors. Personnel with privileged access to infrastructure management systems such as employees, maintenance workers, subcontractors, represent an often-underestimated risk surface. Cases of compromise from within have shown how a single entity with access to control systems can cause damage of comparable magnitude to complex external operations. This profile is particularly relevant in the installation and maintenance phases, where access perimeters are by nature more permeable⁴⁸.

Digital mercenaries. Groups of professional hackers operating on behalf of third parties, typically state actors who want to maintain *plausible deniability*, with high technical skills and objectives defined by the client⁴⁹.

The distinction between state and non-state actors is often artificial. In fact, many non-state actors act on state commission, receive capacity or cover from governments, or operate in a gray space of tacit tolerance by national authorities. The most dangerous category combines state-level technical capabilities with the organization of private entities, maximizing the ambiguity of attribution.

3.4 Vectors and modes of action

Once the actors have been defined, it is necessary to define the means through which the threats are applied. In this sense, it is necessary to distinguish between physical, cyber and geoeconomic vectors.

3.4.1 Physical Dimension

Sabotage. The fundamental factor influencing the methods of physical attack is the depth of installation of the infrastructure. In shallower waters, it is possible to reach

⁴⁵ The term "hacktivism" derives from the combination of the words "hack" and "activism" and is used to indicate that type of hackers who act because they are driven by their political or social dissatisfaction with certain events.

⁴⁶ Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), ch. 18–20; Aanonsen, "Stuxnet, revisited (again): producing the strategic relevance of cyber operations," pp. 72–74.

⁴⁷ ENISA, *ENISA Threat Landscape 2024*, pp. 42–60; Buchanan, *The Hacker and the State*, pp. 48–52.

⁴⁸ Canadian Centre for Cyber Security, "Cyber Threat Bulletin: Iranian Cyber Threat Response to US/Israel Strikes," February 2026.

⁴⁹ Buchanan, *The Hacker and the State*, pp. 70–85; Rid, *Active Measures*, pp. 400–420.

and damage cables and pipelines even with less advanced means; operating at greater depths, on the other hand, requires highly specialized underwater assets.

The first vector is the use of divers to apply explosive charges to the pipeline. The practical bathymetric limit for this modality is about 90–100 m, according to the current limits of specialized military divers.⁵⁰ The differences between the attempted sabotage of a cable off the port of Alexandria in 2013 (carried out by three divers with simple breathing apparatus) and the damage to the Nord Stream 2 pipeline in 2022 (which occurred at a depth of about 84 m with special gas mixtures and about 100 kg of equipment) illustrate the different technical requirements depending on the depth.⁵¹

Another method is the deliberate use of mechanical cutting devices, such as anchors. In this case, the same dynamic of accidental damage is used intentionally, with the additional difficulty for the target country to distinguish the voluntary nature of the act, as evidenced by the cases of the Baltic Sea, where the shutdown of the AIS and the reduction of speed near the infrastructure have fueled suspicions without allowing a definitive attribution.⁵² In the Italian context, the cables that cross the Strait of Messina, the seabed of the Strait of Sicily near the coast or the superficial Adriatic stretches are subject to these risks.

The latest case of physical sabotage is represented by using advanced underwater means for depths greater than 200 m. The necessary sensing, mapping and intervention capabilities are available only to a very limited number of state actors. In this sense, the only two actors probably able to interfere with the infrastructure on the seabed at such depths seem to be the USA and Russia, with the specialized submarines mentioned above.

In addition to these techniques currently in use, it is also good to consider attack methodologies that are currently under development and that could have a reasonably short impact on them. These innovative techniques include bio-adaptive camouflage, camouflaged weapons, armed robots, armed animals, acoustic concealment against sonar detection, geo-engineering of the environment, bio-technological manipulation (including synthetic biology), and increasing the ability of divers to operate in extreme conditions thanks to biological enhancement tools. All technologies that could significantly increase the impact of sabotage actions.

Interception. Data interception by *tapping* specifically concerns communication cables. Contrary to what is generally believed, fiber optic transmission can also be subject to *eavesdropping*, through fiber manipulation techniques, such as fiber bending, evanescent coupling, V-cutting and Bragg grating scattering.⁵³ The goal is to pick up a portion of the optical flow without visibly interrupting communication.

These procedures are easier to perform on the *dry plant*, where a hostile actor can access the cable without physical difficulties. The documented case of the CLS on the

⁵⁰ N. A. (2025), 'Eckernförde: Mine divers extend diving depth to 84 metres', *Marine Forum*, <https://marineforum.online/en/eckernfoerde-mine-divers-extend-diving-depth-to-84-metres/#:~:text=In%20response%20to%20the%20tense,Photo:%20U.S.%20Navy>

⁵¹ For more on the reconstruction of the sabotage at Nord Stream, see: Struckmeier, L. (2024), "How did divers manage to blow up the Nord Stream pipeline? We went down to the spot to find out", *CBC News*, <https://www.cbc.ca/news/investigates/nord-stream-pipeline-explosion-ukraine-diver-1.7296527>

⁵² Kärmas (2024), 'Balticconnector case more sabotage than an accident, experts say', *EER News*, <https://news.err.ee/1609255413/balticconnector-case-more-sabotage-than-an-accident-experts-say>

⁵³ For an explanation of such techniques, see: Iqbal M. Z., Fathallah H., and Belhadj N. (2011), "Optical fiber tapping: Methods and precautions." *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, pp. 164–168.

British coast, intercepted by GCHQ, is the best-known example. In *the wet plant*, the technical capabilities required increase considerably: the Russian specialized submarines of the GUGI and the US submarine USS Jimmy Carter seem to be the only underwater platforms capable of carrying out such operations. Repair ships, which house chambers into which a portion of cable can be introduced, are also considered possible threats to data interception, to the point that Washington has warned its big tech companies of the dangers of relying on Chinese repair companies.⁵⁴

Attack on cable-laying vessels. Repair and installation vessels are another potential point of exposure: their extremely limited number means that damage to even a few of them drastically reduces the responsiveness of the entire system. For example, the entire area of the Mediterranean, the Red Sea and the Black Sea is covered by only two repair vessels.⁵⁵

Cable-laying ships can be hit both in port and during operations, when they are forced to remain stationary. The Somali case of 2016, in which a cable-laying ship was attacked by pirates in the Red Sea, managing to repel the boarding attempt only thanks to the security personnel on board, demonstrates the concreteness of this threat.⁵⁶

3.4.2 Cyber dimension

The most effective way to compromise an underwater network is not to cut the cable: it is to prevent those who manage it from understanding what is happening and intervening in time. The operational objective is almost never immediate destruction, but *recovery drag* (the lengthening of the time between the onset of a failure and its recovery) obtained by degrading the *situational awareness* of operators, altering telemetry, saturating coordination channels or compromising the tools of recovery itself.

Recorded Future, in its State of Security Report 2026, identifies the reversible disruption of cables, satellites and telcos as the coercive tool of choice for state actors: visible enough to signal capabilities, ambiguous enough to remain below the threshold of formal response⁵⁷.

The most relevant cyber-attack vectors for subsea infrastructures therefore include the following scenarios.

Digital supply chain compromise. The digital supply chain is a structure of trust: every node in the chain (firmware vendor, management tool provider, MSP with recurring access) is authorized to interact with the operator's systems. Compromising an upstream node means inheriting that trust, turning a single point of compromise into a multi-target vector.

The European Commission's Cable Security Toolbox (January 2026) explicitly treats the backdoor via EMS/NMS components as a priority threat, with the specific risk of

⁵⁴ Voltz, D. et al. (2025), "U.S. Fears Undersea Cables Are Vulnerable to Espionage from Chinese Repair Ships," *The Wall Street Journal*, <https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320>

⁵⁵ MECMA, <https://www.mecmamc.org/public/index.html>

⁵⁶ Morel, C. (2016), "Threats beneath the seas: Vulnerabilities in the global cable network", *Hérodote*, Vol. 163, No. 4, pp. 33-43

⁵⁷ Martti Lehto, Petro Julkunen, and Hans Hartikainen, "Cyber Security in the Subsea Telecommunication Cable Networks," in ICCWS 2026, pp. 212-221.

malicious system shut down through compromised firmware during the delivery phase. The SolarWinds Orion case remains the documented paradigm: the most relevant effect was not the single intrusion, but the generalized uncertainty about trust in management tools, which forced preventive shutdowns and suspension of remote access in dozens of organizations.

Pre-positioning and persistent access. In this mode, the attacker has no interest in producing any visible effect in the immediate future. The goal is to build persistent and silent accesses on strategic segments of the infrastructure, so as to have options that can be activated in the event of a crisis, a posture that serves as a coercive lever even if those options are never exercised: the adversary knows that they exist and must spend mitigation resources without being able to attribute a concrete threat.

The Volt Typhoon case⁵⁸ documents time-maintained access to critical US infrastructure, including the communications sector, with an institutional reading of risk as "options that can be activated in a Taiwan crisis scenario". In the Middle Eastern context, MuddyWater (MOIS group) conducted through Operation Olalampo (March 2026), a campaign with TTPs indicating shared infrastructure between Iranian actors.

Routing manipulation. The manipulation of BGP (*Border Gateway Protocol*) announcements can be conducted without physical access to the submarine infrastructure and divert traffic through routes controlled by the attacker, allowing massive interception, insertion of malicious payloads or simply degradation of connectivity. The effect can be deliberately "gray": the routes remain advertised, the service remains formally active, but latency, packet loss and instability degrade significantly.

Cases of BGP *hijacking*⁵⁹ (or even hijacking of the *Border Gateway Protocol*, the Internet's routing protocol) associated with state intelligence operations have been documented repeatedly over the last decade. RIPE Labs' technical analysis of cable cuts in the Baltic Sea (December 2024) documents this dynamic with empirical data: following multiple physical cuts, routing resilience reacted asymmetrically, revealing unknown dependencies and logical bottlenecks *ex ante*, confirming that resilience is not only physical but also logical.

Landing hub compromise. The *Cable Landing Station* (CLS) is where the submarine section becomes operable. It houses the cable termination and *Submarine Line Terminal Equipment* (SLTE), powers *repeaters* along the way, concentrates the terrestrial backhaul, and exposes an Internet-accessible Remote Network Management System (RNMS) for remote maintenance.

Malicious access typically occurs through the most ordinary vectors of the threat landscape: exploitation of exposed or out-of-date systems, abuse of service credentials shared between vendors, pivoting from the IT network to management environments, compromise of third-party remote access. In 2022, Homeland Security

⁵⁸ CISA (2023). The Attack on Colonial Pipeline: What We've Learned. Available on: <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned>.

⁵⁹ The term hijacking indicates an attack technique that consists in appropriately modifying certain attributes of a Client-Server communication aimed at directing the victim to malicious resources or, vice versa, to convey the legitimate communication flow between resource and victim to the attacker. See: <https://www.sicurezza nazionale.gov.it/cosa-facciamo/innovazione-consapevolezza-digitale/tipologie-di-attacco/hijacking>

Investigations disrupted unauthorized access to the systems of a private company operating on a critical cable for connectivity in the Pacific, confirming that landing points are attractive surfaces of action even in the absence of kinetic escalation.

Compromise of the management plan. The Kyivstar case illustrates what it means to compromise the nervous system of a telecommunications infrastructure. In December 2023, Sandworm (GRU 74455) activated an access maintained for at least six months within the systems of Ukraine's largest mobile operator, deleting thousands of virtual servers and PCs and disrupting services for 24 million users⁶⁰.

For submarine cables, the risk structure is similar. NOCs, OSS/NMS platforms, telemetry systems and orchestration tools are the level from which fault *detection*, *shunt fault localization* and *dispatch* of repair ships are governed: if this level is compromised, a physical failure turns into a prolonged crisis. The SolarWinds Orion case (*supply chain compromise* of a network management platform that has guaranteed persistent access to thousands of organizations) remains the most documented reference of how hitting management tools produces systemic and lasting effects⁶¹.

Harvest now, decrypt later. As in many other industries, there is a future risk that already has repercussions in the present: the quantum attack. This is currently one of the most underestimated risks. Not so much as an immediate threat, as the technology to decrypt encrypted communications in real time via quantum computers is not yet available, but rather as a strategy for systematically collecting encrypted data to be decrypted later, when post-quantum cryptography will be accessible to attackers.

This approach is adopted by state actors with the necessary storage capacities and makes it urgent to migrate critical infrastructure to post-quantum algorithms, as well as the development of *crypto-agility* capabilities, i.e. the ability to quickly update cryptographic algorithms in use⁶².

3.4.3 Geoeconomic dimension

Alongside the risks described, another type of threat related to the geoeconomic dimension emerges. Submarine infrastructures are located at the intersection of economic, geographical and political-strategic factors. The interpretative framework of "*weaponized interdependence*" developed by Farrell and Newman describes how highly interconnected global networks can be exploited by states as instruments of power. Farrell and Newman identify two main mechanisms: the *panopticon* effect and the *choke point effect*⁶³.

⁶⁰ SentinelOne (2024). Sandworm/GRU 74455 – Kyivstar attack timeline. Available on: <https://www.sentinelone.com/blog/sandworm-kyivstar/>.

⁶¹ GAO, GAO-22-104746 (2022). SolarWinds Orion supply chain compromise — impact on critical infrastructure. Available on: <https://www.gao.gov/products/gao-22-104746>.

⁶² NIST (2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards, August 13, 2024.

⁶³ Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79.

Panopticon effect ⁶⁴. This effect comes from the ability to surveillance and interception that can be exercised through the control of telecommunications infrastructure. An operator who owns or operates an underwater cable potentially has access to all traffic passing through it.

This surveillance capability explains the competition for control of global backbones. In the last decade, the concentration of the underwater cable market has passed into the hands of a few large companies, mainly American *hyperscalers* such as Google, Meta, Microsoft and Amazon (which together control about 69% of global capacity).⁶⁵ These companies have transformed from simple customers to main investors and owners of infrastructure, reducing the role of national telcos. It is currently difficult to design a new subsea infrastructure without their participation.

As anticipated, the danger of data interception does not come only from the operating companies, but also from those in charge of construction and installation: in these phases, devices could be installed to intercept data in transit.

The gradual exclusion of Chinese operators from new cable projects in the Atlantic routes and in the Indo-Pacific corridor derives precisely from the potential danger of a panopticon effect: the Chinese HMN Tech has built and installed several infrastructures, raising concerns about data security, similar to those already emerged for Huawei in the case of 5G.

For Italy, which is a transit hub for cables connecting Europe, the Middle East and Africa, this dimension has direct implications for national digital sovereignty.

Choke-point effect. It consists in the possibility of blocking, limiting or manipulating data or energy flows by exploiting the control of obligatory crossing points. Infrastructure networks have geographical *chokepoints* that give states with strategic positions significant leverage. For example, Egypt is a crucial hub for cables between Asia and Europe and more generally 90% of Europe-Asia traffic transits through the Red Sea/Bab el-Mandeb: this concentration configures a strategic dependence in which the interruption of a single node produces systemic effects on a global scale.

The *choke-point* effect can affect resilience in the maintenance and repair phases. Coastal States retain the right to regulate access to their territorial waters for ships specialized in cable repair: they can therefore deny or delay permission to access repair ships, request inspections, impose operating conditions that slow down interventions.

This mechanism, apparently technical and procedural, can turn into a highly effective tool of political pressure. A recent example is what happened in Yemen, where the fragmentation of political authority slowed down the repair operations of the AAE-1 cable in the Red Sea: the overlap between the claims of the Houthis and those of the internationally recognized government has hindered for months the issuance of the necessary authorizations for the entry of repair ships, with significant effects on the

⁶⁴ The concept originates from the Panopticon, an ideal prison designed in 1791 by the English philosopher and jurist Jeremy Bentham. The key concept is invisible and total surveillance: a circular structure with a central tower allows a single warden to observe all the prisoners, without the latter being able to understand when they are being controlled.

⁶⁵ Salgado, R. (2024), *Undersea Cables, Hyperscalers, and National Security*, Hoover Institution, Stanford University, Aegis Series Paper No. 2304

connectivity of a large geographical area.⁶⁶ The dependence of underwater infrastructures on physical access to the territorial waters of third countries for maintenance operations is a structural vulnerability that cannot be eliminated through technical measures, but only through preventive diplomatic and cooperation agreements.

3.5 Risk mapping

The analysis of the actors, vectors and phases of the infrastructure life cycle converges in the construction of a risk matrix that allows us to systematize the identified vulnerabilities and to orient the response priorities. The matrix is divided into two main axes: the probability of occurrence (from low to high, depending on the historical frequency of events and the availability of the necessary capacities) and the severity of the impact (from limited to systemic, depending on the extent of the effects and the recovery time).

⁶⁶ Leccese, G. (2025), "Chokepoint Above and Below the Surface: The Red Sea's Emerging Infrastructure Challenge", *Istituto Affari Internazionali (IAI)*, IAI Briefs, no. 8, <https://www.iai.it/it/pubblicazioni/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge>

Carrier	Governance & Design	Construction	Installation	Exercise	Repair & Maintenance
PHYSICAL Sabotage · Tapping Naval Attacks	At this stage there is still no physical dimension on which any hostile actors can act.	Possible insertion of backdoors and spy devices (in the case of communication cables), but a problem more related to the cyber and geoeconomic dimension.	Kinetic attachments to cable-laying vessels during installation operations or in port. ► State (navies) + non-state (Houthis, piracy, etc.)	Sabotage and tapping (for communication cables) with different carriers based on depth and infrastructure portion (wet/dry plant). (Anchor dragging in the Baltic Sea 2022-2025, Operation Tempora, 2013) ► State (navies, intelligence services) + non-state (shadow fleets, militias and terrorist groups)	Kinetic attacks on repair ships during operations (Somalia 2016) or in port ► State (navies) + non-state (Houthis, piracy, etc.)
CYBER IT/OT Compromise Digital Supply Chain Pre-positioning	HW/SW supply chain; EMS/NMS backdoor (SMW6/PLCN) ► State (PLA/MSS, HMN Tech)	Compromised firmware; trojanized update (SolarWinds) ► State + Digital Mercenaries (Proxies)	CLS Remote Access; credential theft (HSI 2022) ► State; IAB/ cybercrime organiz.	Management plane; pre-positioning (Volt Typhoon; Kyivstar) ► State (GRU Sandworm, PLA Volt Typhoon, IRGC MuddyWater)	NOC/dispatch; recovery drag; wiper coordination ► State (priority); ransomware-as-a-service (non-stat.)
GEO- ECON. Permits · Choke point Weaponized interdependence Supply chain control	Veto on routes; vendor exclusions (HMN Tech/SMW6) ► State (PRC/USA)	Market concentration; dependence on strategic vendors ► State (nationalized companies or under indirect state control) + economic actors (large suppliers)	Installation permits; diplomatic levers (geographical choke points). Possible positioning of backdoors and spy devices during operations. ► State-owned (coastal states; EEZ leverage)	In the case of communication cables, domain hyperscalers on information flow (Google, Meta, Amazon) ► State (nationalized companies or under indirect state control) + economic actors (hyperscalers)	Permits for access to territorial waters. Possible positioning of backdoors and spy devices during operations (communication cables). ► State (fleet control); non-state (private logistics)

Table 1. Risk matrix for subsea infrastructure

The risk categories that emerge as priorities for the Italian strategic profile are:

Risk Category	Description	Examples
Risk A — High Probability / High Impact	Events with a high probability of occurrence and serious consequences on critical infrastructures.	- Accidental damage from anchors and fishing nets in shallow seabeds (Strait of Sicily, Channel of Otranto, Adriatic areas) - Pre-positioning cyber-attacks against landing station management systems - Digital supply chain compromise in software update processes
Risk B — Medium Probability / High Impact	Threats that are less likely, but still significant and potentially very damaging.	- Physical sabotage of shallow-water infrastructure by state actors with plausible denial capabilities - Physical attacks or diplomatic interdiction of repair ships in regional crises (Red Sea and Strait of Hormuz) - Damage to cables at global choke points (Suez, Hormuz) due to indirect causes deriving from geopolitical instability
Risk C — Low probability / Systemic impact	Rare events but with the potential to cause large-scale damage and disrupt entire networks.	- Coordinated sabotage of multiple deepwater infrastructure (requires advanced state capacity) - Combined physical-cyber-attack with prolonged disruption across multiple infrastructures - Harvest-now-decrypt-later systematically applied to government and military traffic
Risk D — Variable probability / Moderate impact	Heterogeneous risks with smaller but still significant impacts, including reputational ones.	- Damage from natural phenomena (seismicity, submarine landslides) in geologically unstable areas - Hacktivist or cybercrime operations with limited effects but high reputational impact - Geoeconomic pressures through vendor exclusion in the supply chain

Table 2. Risk Matrix - Impact

Reading the matrix suggests some implications for response policies. The risk of greatest urgency is not necessarily that of greatest potential impact (multiple coordinated sabotage in deepwater), but that of category A: the high-probability and high-impact events that already occur today with documented frequency in other geographical areas, such as the Baltic Sea. The prioritisation of passive protection measures (*hardening*, redundancy), surveillance in coastal areas and the development of rapid response capabilities responds to this priority risk profile. At the same time, C-risk management, which has low probability but systemic impact, requires long-term investments in deterrence capabilities and coordinated response mechanisms at NATO and EU levels, which do not have immediate effects but are indispensable for long-term strategic resilience.

10. Defense Solutions and Protection Models

4.1 Prevention, surveillance and deterrence measures in the underwater context

The protection of critical submarine infrastructures must be framed in an integrated perspective. Too often the focus is on the repair and restoration phase. Instead, the entire life cycle of the infrastructure must be considered to make the safety system truly operational. In this way, the first safety measures must be implemented already in the planning and construction decision phase of the work. Further considerations must be made regarding the supply chain that leads to the construction of the cable. This is followed by assessments on laying at sea, monitoring, deterrence and prevention. Only after these phases is it appropriate to focus on the repair and restoration phase.

Maritime *Domain Awareness* (MDA) is recognized as the most functional doctrine in ensuring the security of maritime space⁶⁷.

Starting from this premise, knowledge of the maritime environment cannot be exhausted in an operation of simple data collection but must extend to a process of "understanding" that transforms information from sensors and human sources into useful knowledge to define adequate protection and response measures. This, from a doctrinal point of view, is presented as fundamental for the so-called *deterrence by detection*, i.e. the ability to detect and attribute anomalous activities more likely, thus discouraging one or more hostile actors from resorting to hybrid tactics.

With reference to the underwater environment, this thought has evolved into the concept of *Underwater Domain Awareness* (UDA). The practical implications of this evolution are different. In the abyss, in fact, the barrier is no longer exclusively for access to data but is first and foremost physical: water is in fact an excellent element in shielding radio and electromagnetic waves.

If in the framework of the MDA the awareness of the maritime domain is largely based on patrolling and monitoring activities (based on technologies operating in the air-maritime space), in the underwater context this first level of surveillance is confronted with a different reality, where these tools meet the physical limits of the aquatic environment.

Therefore, the complexity of the underwater dimension requires a shift from the use of isolated data to the creation of integrated networks that aggregate different technologies, with the aim of making the water column more transparent and better protecting the critical infrastructures that are immersed in it.

On a technical level, the most effective technologies for the UDA doctrine are *sonars*, divided into active and passive, which are the basis of the SDCL-A (*Search, Detect, Classify, Localize to Attack*) operating cycle. The former certainly offer a more accurate localization through the emission of pulses, being more effective for the *Search-Detect-Localize* phase of the SDCL-A cycle along the routes of cables and pipelines,

⁶⁷ Bueger & Edmunds (2024), "Understanding Maritime Security": p. 173

thanks to the ability to generate detailed profiles of the seabed; on the other hand, however, they expose the platform that uses them, revealing their position⁶⁸.

Passive *sonars*, on the other hand, are limited to collecting acoustic signals and are therefore privileged for the *Classify-Localize* phase of the cycle, as they allow for more prolonged and "silent" monitoring of the areas around gas pipelines and cables; their main limitation, however, is represented by possible false alarms caused by ocean background noise and by the lower accuracy in estimating distance and depth. Alongside acoustic sensors, there are also systems based on *Magnetic Anomaly Detection* (MAD), which work by measuring small variations in the Earth's magnetic field due to the presence of metal masses, such as submarine hulls. At the same time, in recent years, more technologies are becoming widespread that use optical sensors and bathymetric *Light Detection and Ranging* (LiDAR) instruments, which allow, through laser technology, to acquire high-resolution three-dimensional models of pipes and cables on the surface of the seabed. They make it possible to identify structural deformations, local erosion and, with respect to the more strictly defense aspects, signs of physical manipulation⁶⁹.

The effectiveness of detection technologies, however, depends on the platforms through which they are deployed and used operationally. In the past, the instrument par excellence of the underwater environment were submarines, whose use in recent decades has undergone a strong paradigm shift in the maritime security strategies of States: from strategic deterrents for their capabilities to launch intercontinental ballistic missiles, as well as for being the main assets for anti-submarine or anti-ship warfare, they have progressively evolved into a multi-domain key⁷⁰. As can also be seen from the development of the next Italian U212 NFS or the Swedish A26, submarines are now designed to project combat power, collect information and direct actions in the air, on the surface, in space, in cyberspace and in the electromagnetic spectrum.⁷¹ In this sense, in addition to acting as nodes in a network of underwater and non-underwater sensors, these will have to be able to function as "mother ships" for unmanned systems such as ROVs and AUVs. In fact, these unmanned systems provide several advantages and opportunities for the protection of underwater infrastructures: in the case of AUVs, these can perform planned routes over large areas, collecting information on the status of infrastructures along pre-established routes; while ROVs are useful for use aimed at close inspections and direct interventions on cables and pipelines, thanks to equipment consisting of high-definition cameras and operational arms⁷².

Finally, in the long term, a significant change with respect to these means will concern the evolution of operational capabilities through Artificial Intelligence models. The most recent studies on the application contexts of AI in the underwater environment highlight some priority lines of development, including an improvement in decision-making autonomy, both with reference to the paths to be crossed and in the ability to choose the objectives of the mission, if not even to identify the *target*⁷³. This responds

⁶⁸ Sensors (2025), *Route Optimization for Active Sonar in Underwater Surveillance*, p. 2

⁶⁹ Milan Vego (2019), *Maritime Strategy and Sea Denial*, p. 112

⁷⁰ CeSI (2024), *The (almost) submarine domain*, p. 45

⁷¹ Fincantieri, "U212 NFS", <https://www.fincantieri.com/it/business/prodotti/navi-per-la-difesa/sommergibili/u212nfs>; Saab, "The world's first 5th-generation submarine", <https://www.saab.com/products/5th-generation-submarine>

⁷² European Commission Expert Group (2026), *Security and Resilience of EU Submarine Cable Infrastructures*, p. 9

⁷³ Leonardo Foundation (2023), *Civiltà del Mare Report*, pp. 34-36

to the need to circumvent communication problems with those on the surface, which is often limited or even absent.

Beyond technological advances, the effectiveness of these systems continues to depend on human capabilities: the process of data collection and analysis loses its importance if it is not integrated into efficient command and control systems capable of aggregating the information received from different agencies and institutions, through a process called "interagency".⁷⁴

Consequently, perhaps an even more significant limitation than technological ones is of a social nature: we refer to the unwillingness of organizations involved in maritime security to share information with each other, which is found even between agencies and public institutions belonging to the same institutional security framework.

Furthermore, a similar dynamic also emerges in relation to the relationship between public and private, which is also essential to achieve effective protection of underwater infrastructures⁷⁵.

The high costs of design, development and integration have, at least so far, limited access to the underwater dimension to a few technologically advanced powers, also making the presence of non-state actors organized in this operational dimension extremely rare⁷⁶. However, in the medium to long term, it is likely that in the medium to long term these systems will begin to spread in a similar way to what happened for aerospace drones: miniaturization, cost reduction and the transfer of *know-how* to a wider number of actors will therefore make the observation, intrusion or manipulation capabilities of underwater infrastructures accessible to a growing number of states, *proxy actors* and non-state entities. As a result, this proliferation process will increase the complexity of hybrid threats and make the challenge of *deterrence by detection* even more challenging, giving even more crucial importance to UDA systems.

4.2 Passive protection and infrastructure resilience

The protection of critical underwater infrastructures cannot be based solely on the ability to detect hostile activities, as it is difficult to imagine that in the short term it will be possible to achieve total protection from possible threats in such a vast environment as the underwater one. This is why, alongside deterrence and surveillance measures, the development of passive protection strategies and resilience of infrastructures plays a role of primary importance when discussing seabed protection⁷⁷.

In this context, the first rule of a process that does not allow the continuity of the service to be significantly interrupted by damage concerns the ability of a network to redistribute flows, i.e. divert them to alternative routes, thus absorbing the interruption of one or more segments without collapsing⁷⁸. In fact, the concept of route diversification refers both to increasing the number of cables and to avoiding excessive

⁷⁴ Critical Maritime Infrastructure Protection: What's the Trouble? (Bueger & Liebetrau, Marine Policy 155), p. 6

⁷⁵ Why Adversaries Target CUI and Challenges in Protection (in WHY-CUI-IS-THE-TARGET.pdf), p. 3.

⁷⁶ The threat to the submarine infrastructures of the "Enlarged Mediterranean". The means and possible techniques, pp. 2, 4. (Art-R.M.-su-Minaccia-CUI.pdf)

⁷⁷ Critical maritime infrastructure protection: What's the trouble? , 2023, p. 6

⁷⁸ Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure (UNIDIR), p. 10

concentration along the same trajectories, if they are at high risk of accidental damage or of a geopolitical nature. Geographical diversification, in addition to responding to quantitative criteria, therefore also uses qualitative criteria that refer to the distribution of perceived risk.

From an economic point of view, however, both the redundancy of cables and the diversification of landing points and interconnections may not be economically viable for private operators⁷⁹. This must be taken into account because economic needs can create contrasts between the private and public sectors: the latter, in fact, can only primarily enhance the continuity of the service, beyond the costs, since most of the essential services of a State depend on it, including the components of national security themselves.

A further level of protection is achieved when an interruption of the service is made materially more difficult (and therefore less likely); this can be done through physical protection of the infrastructures located on the seabed. The most immediate example is the burial of cables in the seabed. However, it is useful to point out that there is no standard *hardening* solution applicable indiscriminately to all contexts, because effectiveness depends on the geological characteristics of the different seabeds, as well as on the nature of the threat to be prevented. Furthermore, a greater depth of burial does not always equate to a proportional increase in the safety of the infrastructure. In fact, the possibility of unexpected failures and the consequent repair or replacement operations must be considered. On a technical level, a compromise must therefore be found, i.e. a balance between protection and the need for maintenance. In addition to burial, a further measure of passive protection is represented by *armoring*, i.e. the physical strengthening of the cable in the sections most exposed to shocks, abrasions or other unpredictable kinetic ⁸⁰traumas.

Finally, *hardening operations* include some apparently less "material" but equally important measures in the context of passive protection, such as the establishment of the so-called "*cable protection zones*".⁸¹ A measure such as the latter makes it possible to avoid many of the possible accidental damage and at the same time is one of the most properly defensive strategies against possible hostile actors, who are denied access to the area of interest.⁸² However, the counterpart of this type of measure is the risk of excessively limiting some essential economic activities (e.g. fishing). Therefore, even measures such as these must follow a logic of balance between defense and actual risk.

Finally, the concept of resilience can be configured as the set of actions aimed at maintaining essential functions, albeit in a degraded form, following an event (whether deliberate or accidental) that puts the system in crisis. In this context, business continuity therefore constitutes a point of connection between the concepts of passive protection, emergency management and restoration of functionality, making it possible

⁷⁹ The diversity, frequency and severity of natural hazard impacts on subsea telecommunications networks, p. 14

⁸⁰⁸⁰ The diversity, frequency and severity of natural hazard impacts on subsea telecommunications networks, 2024, p. 14

⁸¹ Enhancing the Resilience of the Global Submarine Cable Ecosystem (CCPL, 2025), p. 21

⁸² Cable protection zones are "geographical areas, identified and proclaimed by coastal states, within which certain activities are reduced or prohibited, capable of damaging submarine cables [...]". Nigro, E. (2024), "Submarine Cables between Legal Problems and Space Problems", *Transport Law Review*, Year XXXVII n. 1, <https://www.dirittodeitrasporti.it/app/uploads/2024/06/IV.-Nigro.pdf>

to transform vulnerability into manageable damage, rather than systemic paralysis⁸³. This implies the presence of protocols capable of ensuring timely reporting of the event and the activation of coordination between the operational level and the political-administrative level⁸⁴.

However, the maintenance of essential functions is as much a matter of technology as it is of *governance*⁸⁵. This is true both in peacetime, with interruptions resulting from accidental events, and in ambiguous or openly conflicting scenarios. In fact, business continuity must be thought of as the ability to cross the entire time interval that separates the moment of damage from the recovery of the system and not only the moments immediately following the interruption.

4.3 Response and Recovery Following Disruption

When an event occurs that interrupts the flows of energy or data flowing through the seabed, it is essential that a well-defined rapid response process is initiated. Following the reporting of the failure, a preliminary assessment is therefore essential, which allows information to be collected from the first moment on the type of interruption, whether it can be considered of a malicious nature, as well as on its possible cross-border impact, so as to be able to alert neighboring and allied countries. At this stage, the preliminary assessment can also be guided by some operational indicators, such as the presence of potentially hostile, flagged ships in anomalous stops near sensitive routes, or the deactivation of AIS systems as well as other irregular navigation behavior. While it is true that these elements cannot be considered sufficient in themselves to demonstrate hostile conduct, they nevertheless give a more precise idea of the probability that the event is plausibly accidental or an episode compatible with sub-threshold sabotage.

The initial response process, in parallel with the information reconstruction operation, also requires rapid securing of the most accessible and/or vulnerable segments of the infrastructure. It follows that, especially in contexts where deliberate damage is assumed already in the first hours after the event, the response must include access control measures and protection of coastal sites, to prevent further vulnerabilities from being added to the initial interruption.

The first problems of attribution acquire a non-negligible political-strategic importance. It follows that the event has a real political significance, which influences the type and degree of response mobilized by national authorities, or if necessary, taking the Euro-Atlantic context as an example, multilateral cooperation frameworks. In today's context of renewed international competition, the protection of underwater infrastructures is increasingly considered a matter of coordination between national authorities, the European Union and NATO, especially in cases where it is difficult to distinguish between an accidental disruption and a deliberate threat by a hostile actor.

Regarding the Atlantic Alliance, there is often a tendency to place it in a strategic framework of deterrence and military response. On the other hand, the EU moves more

⁸³ Critical Infrastructure Protection, Risk Management, and Resilience (Pesch-Cronin & Marion, 2024), pp. 11, 14

⁸⁴ Maritime Critical Infrastructure Protection (MCIP), MARSEC COE, 2023, pp. 14-15

⁸⁵ Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure, UNIDIR, 2025, pp. 41-42

on a terrain of *governance* of critical dependencies, therefore closer to regulation and the concept of resilience.

The difference between the two entities also emerges from the strategic formulas referred to in official documents: while NATO is often reduced to the logic of "*prepare, deter, defend*", the European Union's approach is more easily summarized in terms of "*awareness, resilience, response*".⁸⁶

However, this dualism on the European continent is not without friction, which in fact emerges in what risks leading to a functional overlap rather than a necessary complementarity, also due to the different institutional nature of the two organizations.

The management of a crisis involving one or more submarine infrastructures is therefore presented as a test bed for the Euro-Atlantic ability to create a single security architecture.

In an ambiguous context, there is not simply a problem with respect to "who is in charge": the pressure exerted on society takes on more value, from an operational point of view but also from a political and symbolic point of view. Consequently, institutional communication is a fundamental tool, the underestimation or lack of which risks aggravating the situation. Quickly communicating that response procedures have been activated and that restoration is underway can help both to reassure users and to contain the risk of *escalation* and loss of institutional credibility.

Communication can therefore be defined as truly effective if it becomes an element of stability of the institutional structure, removing the risk of spreading a perception of loss of political control. It can therefore be argued that the management of a crisis, in the underwater dimension, requires a double credibility: operational, linked to the speed and consistency of coordination between the actors involved, and narrative, i.e. the ability of the institutions to present the fact as the object of an orderly response and not of an improvised reaction.

4.4 The Repair Process

Remediation techniques constitute the conclusive, but also most concretely verifiable, segment of the entire incident response chain.

In fact, after the section to be repaired has been identified, a reflection is started on what is the best technique to intervene. This type of activity requires the use of unmanned ROV platforms or, in shallower sections, the possibility of involving specialized divers. An element that takes on particular importance is therefore the actual availability of these capabilities. Some reports point out that until 2025 there were about eighty ships suitable globally, but often constantly engaged in laying new routes, with obvious repercussions on the possibility of intervening quickly in the event of breakdowns⁸⁷. In fact, it is hoped that breakdowns will always remain manageable

⁸⁶ NATO, Baseline Requirements for the Protection of Critical Undersea Infrastructure (Brussels: NATO, 2023), pp. 12–17. See also EU Expert Group, Cable Security Toolbox, measure TM03, pp. 21–24

⁸⁷ Runde, D. F., Murphy, E. L., & Bryja, T. (2024). Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition. Center for Strategic and International Studies

within an ordinary threshold: if in a context of open conflict these infrastructures were targeted more massively, all the limits of a system unable to withstand such an eventuality would emerge. In this scenario, in fact, the criticalities caused by multiple competing failures would quickly saturate the already limited response capabilities.

In addition to the point of view of capabilities, repair processes have repercussions that touch on the level of law and diplomacy. As anticipated in the previous chapter, geopolitical factors have their influence, for example regarding the access of repair ships to the territorial waters of different states. Another element concerns the possibility for public institutions to have the skills and means necessary for intervention, which favors a faster process disconnected from the dynamics of business and international politics.

Once again, these issues, although highly technical, tend to flow naturally into the context of political-institutional coordination.

11. Foreign experiences

5.1 United States

The United States exercises global leadership in the underwater dimension thanks to the offensive capabilities of the Cyber Command, which operates according to the Defend Forward doctrine, and advanced naval surveillance systems, including the Mainsail system for tracking the Russian shadow fleet. However, governance is fragmented between DHS (Department of Homeland Security) - CISA (Cybersecurity and Infrastructure Security Agency), DoD (Department of Defense), DoS (Department of State) and FCC (Federal Communications Commission), in the absence of a dedicated centralized agency. The main structural paradox is that 69% of global cable capacity is controlled by private American hyperscalers, making the protection of critical infrastructure inherently dependent on public-private cooperation⁸⁸. The most critical bottleneck is repair capacity: only two specialized ships operate under the American flag out of a global fleet of 65-80 units, a vulnerability explicitly recognized by DHS and not yet solved⁸⁹.

5.2 France

France is the only European country that combines regulatory, industrial and military sovereignty in the underwater dimension, representing the reference benchmark for Italy. Orange Marine manages 15% of the world's fleet of cable-laying vessels (6 units, operational within 24 hours) and Alcatel Submarine Networks (ASN), 80% nationalized, adds a further 6 ships with 650,000 km of cables laid worldwide: a Base Industrielle et Technologique de Défense with no equivalent on the continent. The military doctrine "know, monitor, act" is operationalized by the CEPHISMER cell of the Navy, with AUVs and ROVs operating up to 6,000 meters⁹⁰. The regulatory framework has been shifted from civilian to security, with severe penalties for damaging infrastructure and strengthened control over underwater drones. The main point of attention is the concentration of 8-13 intercontinental cables on the Marseille hub, which configures a potential single point of failure for European connectivity⁹¹.

5.3 Japan

Japan has developed the most systematic and integrated approach in Asia, combining centralized governance (Cabinet Secretariat, National Security Secretariat), sovereign industrial capacity and multilateral projection. With an estimated share of around 30% of the global market for cable laying and repair vessels and state subsidies of up to 50% for the acquisition of new units⁹²; Tokyo is the only credible competitor to French dominance in this sector. On the multilateral level, it leads the Quad Partnership for Cable Connectivity and Resilience and the capacity building program towards Pacific

⁸⁸ Abels, J., & Babić, M. (2026). Cable wars? Mapping the political economy of submarine cables in an era of geoeconomic competition. Globalizations

⁸⁹ Mahle, M. B. (2025). Subsea cables and US national security. Steptoe LLP

⁹⁰ Secrétariat général de la mer. (2022). L'économie bleue en France - Édition 2022

⁹¹ lanc, F. (2018, June). Géopolitique des câbles : une vision sous-marine de l'Internet. Centre pour la Technologie et la Société, Département de droit, Fundação Getulio Vargas.

⁹² Cybersecurity Strategic Headquarters, Government of Japan. (2024). The cybersecurity policy for critical infrastructure protection.

Island states as part of the Free and Open Indo-Pacific vision⁹³. The Yokohama Zone agreement guarantees regional coordination for emergency interventions. The reference threat, explicitly identified, is the combination of Russian and Chinese capabilities in the underwater dimension of the Indo-Pacific.

5.4 Australia

Australia has built the most mature regulatory framework among English-speaking countries: the Cable Protection Zones established by the Telecommunications Act 1997 limit navigation, fishing and anchoring in the corridors adjacent to landing points, and the Critical Infrastructure Risk Management Program imposes binding obligations on private operators. Governance is coordinated by the Department of Home Affairs with the Australian Signals Directorate for the cyber dimension. The main structural gap is the lack of a national cable repair ship: in the event of an accident, Canberra depends entirely on international operators, with intervention times that cannot be controlled, a vulnerability explicitly recognized but not yet resolved in strategic assessment documents⁹⁴.

5.5 Sweden

Sweden has radically transformed its posture after 2022, elevating the protection of critical maritime infrastructure (CMI) to a national security priority under the Total Defence (Totalförsvar) model, which integrates civilian and military dimensions. NATO membership has turned the Baltic into an "allied lake" and enabled participation in the Baltic Sentry mission and Operation Nordic Warden (JEF), which uses AI systems for real-time monitoring of the Russian shadow fleet. Governance is centralized at the Swedish Civil Contingencies Agency (MSB). Stockholm, like Australia and Ireland, also lacks a state-owned fleet of cable-laying vessels, depending on private operators for repair, with additional operational complications related to the winter conditions of the northern Baltic.

5.6 United Kingdom

The UK has one of the world's most extensive submarine cable infrastructures in the Northeast Atlantic and a significant naval defense industrial base. The Joint Maritime Security Centre (JMSC) ensures inter-agency coordination between the Royal Navy, Coast Guard and civilian operators, with the NCSC responsible for the cyber dimension. Astute-class submarines perform surveillance and intelligence functions in strategic areas. Participation in AUKUS projects cooperation on advanced submarine technologies, including next-generation AUVs, with USA and Australia. The focus is the reliance on international private operators for deep-sea repair operations.

5.7 Ireland

⁹³ Cannon, B. J. (2025). Undersea cable security in the Indo-Pacific: Enhancing the Quad's collaborative approach. *Marine Policy*, 171, 106415.

⁹⁴ Bashfield, S. (2025). Defending seabed lines of communication. *Australian Journal of Maritime & Ocean Affairs*, 17(4), 557-569

Ireland embodies the most marked paradox on the European landscape: about three-quarters of the Northern Hemisphere's submarine cables transit through or near its waters, with daily financial transactions estimated at \$10 trillion, but maritime security has long remained understaffed. Nord Stream (2022) has acted as a catalyst: the country is centralizing competences under the Department of Defense, with a new Maritime Security Unit and the Maritime Area Regulatory Authority. The total reliance on private repair consortia and the absence of autonomous surveillance capabilities of the EEZ, ten times larger than the national land mass, remain the most urgent structural vulnerabilities.

5.8 Israel

Israel has a profile of extreme maritime dependence: 99% of foreign trade transits by sea, the energy mix is composed of 44% offshore natural gas and 39% oil, and submarine cables, including the JONAH cable (2,300 km, Tel Aviv-Bari), constitute the only viable digital connection with the rest of the world, given the impossibility of developing land routes for geographical and geopolitical reasons. The country is therefore often described as "a strategic island", with three primary maritime risk routes: the Suez Canal, the Strait of Tiran and the Mediterranean routes adjacent to hostile areas (Libya, Syria, Maghreb). The protection of offshore gas fields is the top priority of Israel's maritime security agenda, in a threat framework dominated by Iran and its regional proxies (Houthis, Hezbollah). The governance of critical underwater infrastructures is distributed and lacks a centralized authority: the *National Security Council* coordinates strategic planning, the *Israel Security Agency* and the *National Cyber Directorate* manage threat monitoring, while the private sector, led by Bezeq and Exelera, operates largely independently of government bodies. On the operational level, Israel does not have national cable repair capabilities (the 2024 post-attack repair was delegated to the Italian E-marine) and is focusing on multilateral cooperation to bridge the gap: emblematic is the trilateral agreement with Cyprus and Greece for the establishment of the *Joint Maritime Cybersecurity Centre of Excellence* (MarCCE), dedicated to monitoring cyber-threats and the coordinated development of operational capabilities.

5.9 China

China operates simultaneously on three levels: military (APL Navy with increasing Atlantic projection), commercial-industrial (HMN Technologies/formerly Huawei Marine Networks in tenders for new cables) and regulatory (Digital Silk Road framework for the creation of favorable infrastructure interdependencies). The combination of physical access to systems in the construction and repair phases and the ability to compromise management systems is the most worrying threat profile for Europe and Italy. HMN's exclusions from projects in Atlantic and Indo-Pacific routes have reduced but not eliminated Chinese penetration in the sector; the difficulty of total exclusion is structural, given the price competitiveness of Chinese operators compared to Western alternatives.

5.10 Egypt

Egypt geographically controls the Suez Canal, a choke point obligatory for more than 90% of data traffic between Europe and Asia, and hosts some of the most strategic landing stations in the Mediterranean in the Alexandria area. Governance is characterized by high state centralization and robust physical security regime, but with limited transparency towards international partners. The Houthi attacks on underwater infrastructure in the Red Sea corridor (2024) have increased pressure on Cairo for greater regional coordination in the protection of transit ridges.

5.11 Turkey

Turkey controls the Bosphorus Strait and the Dardanelles, key choke points for traffic between the Black Sea and the Mediterranean and has centralized the governance of critical infrastructure security under the Presidency of the Republic, with the Presidency of Cyber Security as the digital coordinating authority and the Ministry of Defense for maritime assets. Turkey's rapidly developing defense industry includes AUV and underwater surveillance programs that reduce dependence on foreign suppliers. The posture of strategic autonomy, which maintains relations with all regional actors, including Russia and Iran, complicates infrastructure intelligence sharing with NATO allies, while maintaining full formal interoperability in the Alliance.

6. The underwater dimension to 2050: four futures for Italy

6.1 Why look to 2050, and how.

The previous sections have given a snapshot of a rapidly changing dimension: an expanding physical infrastructure, a threat being structured, a regulatory and capacitive framework under construction. A snapshot, however, ages quickly, and the decisions that the country is called upon to take on the regulatory perimeter, on the Navy's capability investments, on the posture to be taken in NATO and EU formats, will unfold their effects on a horizon measurable in decades, not in budget cycles. For this reason, the present section integrates the analysis with a scenario exercise at the 2050 horizon.

The exercise adopts an openly exploratory perspective: it does not intend to predict what future will be realized, nor to design the desirable future, but to delimit the space of plausible futures within which Italy will have to move, so as to distinguish the robust choices, valid in all futures, from the contingent ones, valid only in some⁹⁵. On the methodological level, the technique of *Alternative Futures Scenarios* was followed, which structures the work in successive phases: census of the factors of change, separation between heavy trends and critical uncertainties, selection (verified through a cross-impact matrix) of the two dominant uncertainties, construction of the four futures resulting from their combination and definition of early warning indicators that allow, over the years, to recognize towards which scenario the system is slipping⁹⁶. The twenty-five-year horizon is not accidental: it is the minimum time for the structural transformations already underway (e.g. the energy transition, the generational renewal of fiber backbones, the maturation of autonomous systems) to be carried out and at the same time the maximum time within which the capacitive choices launched today will produce fleets, sensors and skills that are actually operational.

6.2 What will happen anyway: the predetermined elements.

Before diverging, the four futures share a common ground. In fact, some dynamics have a degree of uncertainty low enough to be considered predetermined elements of any scenario, and it is worth stating them at the beginning because they constitute the underlying load on which critical uncertainties are grafted.

The first is the structural growth in demand: data traffic, driven by cloud services and artificial intelligence, and electricity demand will continue to increase, and with them the number of cables, interconnections and nodes resting on the seabed. The second is the physical expansion of the national exposure area: offshore wind power planned in the southern seas, new electricity interconnections and any new gas import capacity will add kilometers of infrastructure and new landing points to an already extensive perimeter. The third is the persistence of accidental risk (anchorages, trawling, natural

⁹⁵ On the distinction between predictive, exploratory and normative scenarios: Börjeson, L., Höjer, M., Dreborg, K.-H., Ekvall, T., Finnveden, G., "Scenario types and techniques: Towards a user's guide", *Futures*, 38(7), 2006, pp. 723-739;

⁹⁶ For the technique of *Alternative Futures Scenarios* and the related process (definition of purpose and horizon, identification and selection of factors, development and comparison of scenarios, definition of indicators, monitoring and updating), as well as for the use of the cross-impact matrix to support the selection of factors: Valeriani, M., *Intelligence Analysis for Global Politics: Concepts and Techniques to Analyze an Uncertain World*, Routledge, 2025, chap. 6

events) that the matrix of chapter 3 places in the high probability and high impact category and which will grow in absolute value precisely because the exposed surface will grow, regardless of any geopolitical evolution. Finally, the fourth is the technological maturation of underwater sensors: the technical ability to observe the seabed will improve in any case; what remains open is who will own it and with what coverage, and it is precisely here that the uncertainty begins.

6.3 The two critical uncertainties.

From the census of factors conducted based on the previous chapters, two uncertainties emerge that dominate all the others in terms of impact, openness of the trajectory and mutual independence.

The first of a technological-strategic nature concerns the proliferation of underwater operational capabilities. Today, the possibility of acting effectively on the seabed, whether to map, manipulate, repair or sabotage at significant depths, remains an oligopoly of a few navies and a small industrial segment. However, the trajectory of autonomous and remote systems, the fall in costs, the intrinsically dual nature of technologies and the porosity of export control regimes make it plausible, over a twenty-five-year horizon, a real democratization of the threat: long-range underwater drones accessible to minor navies, proxy actors and potentially non-state entities, with effects on attribution that we have already seen is now the Achilles heel of the response, are all aspects destined to worsen. At the other extreme, effective control regimes, persistent industrial bottlenecks and the operational complexity of the deep environment could keep the capacity concentrated. The outcome is not written it is the first dimension of variation.

The second of a political-capacitive nature concerns Euro-Atlantic cohesion and collective capacity in the protection of underwater infrastructures, including its industrial base. The report documented the start of institutional construction, from NATO coordination, to Recommendation (EU) 2024/779 and the European Action Plan on cable safety, which by 2050 may have consolidated into an integrated system of surveillance, deterrence and response, equipped with what is most conspicuously lacking today: a manned industrial capacity for laying and repair, now entrusted to a global fleet of a few dozen specialized units, largely non-European and contended for by growing demand. Or it may have run aground in fragmentation: uncoordinated national initiatives, structural dependence on non-European private operators, starting with hyperscalers, who already control a dominant share of the new fiber capacity, and to which is added an atrophied industrial base just as the surface to be protected expands. Here too, the outcome will depend on political, industrial and budgetary choices still ahead of us. It should be noted that this second dimension is not entirely exogenous: Italy contributes to determining it. Far from being a methodological defect is the very reason for the exercise: in the tradition of *prospective*, the future is not just something that happens, but something that institutions contribute to building⁹⁷.

⁹⁷ On the *prospective* tradition and the anticipation-action orientation of strategic foresight: Coates, J., Durance, P., Godet, M., "Strategic Foresight Issue: Introduction", *Technological Forecasting and Social Change*, 77(9), 2010

The intersection of the two dimensions generates four futures. Each is associated with a synthetic name, an internal logic, the position that Italy would occupy and the indicators that would signal its approach.

The four scenarios are summarized in the image below.

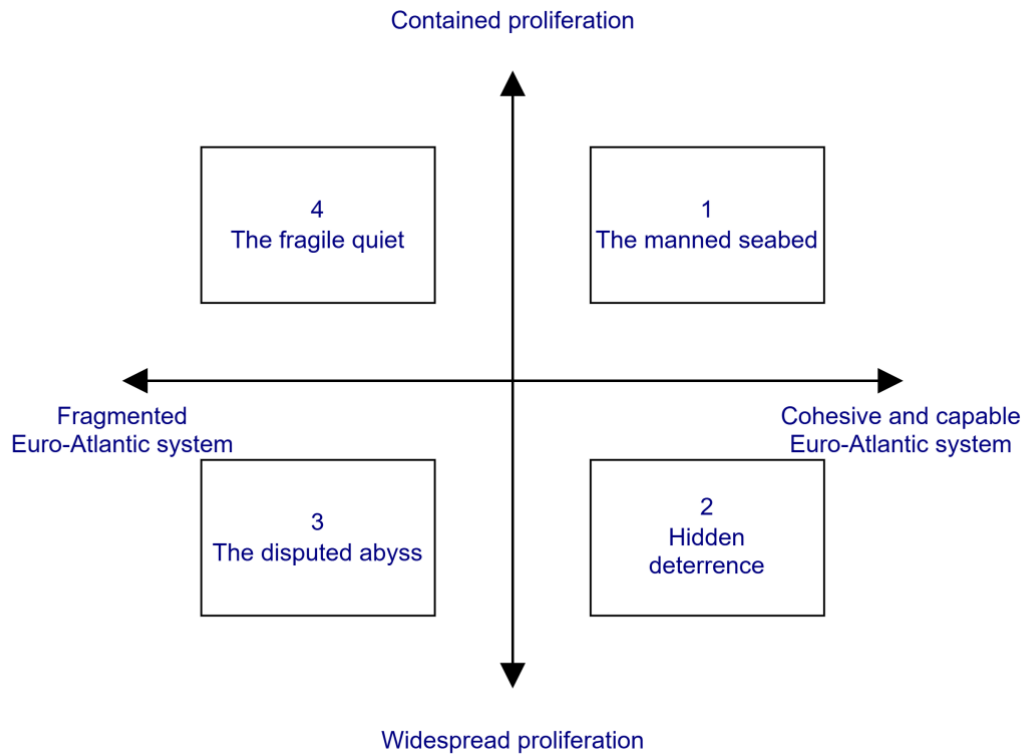


Figure 6: Future scenarios for Italy

6.3.1 First scenario - The manned seabed

Contained proliferation, a cohesive and capable Euro-Atlantic system.

It is the future of successful construction. By 2050, the ability to operate at depth remained the preserve of a few navies, while the Euro-Atlantic system completed its architecture: integrated surveillance of the critical seabed with distributed sensors and allied data fusion, a permanent incident response mechanism, and, a decisive junction, a European fleet of cable-laying and cable-repair ships built in the 1930s through joint industrial programs, which reduced restoration times from weeks to days and took the function away from the spot market. Deterrence operates primarily by detection: the probability of attribution has become high enough to make sabotage a costly option, and the deliberate threat has shifted to the cyber domain, where attribution remains more nuanced.

In this future, Italy has capitalized on its geography: national ports and shipyards host a share of the European fleet, the Navy exercises the role of presiding over the Mediterranean quadrant that Law 9/2026 had foreshadowed, and the cable hub has been consolidated because the perceived safety of the Italian corridor has become a competitive advantage over alternative routes. The dominant risk, paradoxically,

returns to be the accidental risk of category A (anchors and nets), together with a more subtle risk: habituation. A system that works generates the temptation to defund it. A further consolidation of the resilience of this system could also come from investments in infrastructure that increase the redundancy of the overall infrastructure.

Approximation indicators: launch of joint European programmes for cable-laying/cable repair units and Italian participation; growth in the rate of public attribution of accidents; trend reduction in average repair times in the Mediterranean; export control regimes extended to autonomous underwater systems and effectively applied.

6.3.2 Second scenario - Hidden deterrence

Widespread proliferation, a cohesive and capable Euro-Atlantic system.

It is the future of armed surveillance. Technological democratization has been accomplished: long-range autonomous systems are available to numerous navies, proxy actors and non-state organizations, and incidents in the gray area have become a low-intensity constant. But the allied system has held up and strengthened precisely under pressure, as already happened in the Baltic in the mid-twenties: surveillance is capillary, response rapid, redundancy planned. The result is a dynamic and expensive balance outlined by permanent competition between measures and countermeasures on the seabed, logically analogous to the cyber race. A future therefore in which successful attacks do not disappear but remain below the systemic threshold because recovery is fast and redundancy absorbs.

For Italy it is the future of the front line: the Mediterranean centrality, elsewhere an advantage, here means maximum exposure to the traffic of hostile systems directed towards the bottlenecks of Sicily and Otranto, where the new infrastructural load of the energy transition concentrates targets and enemy attention. The Navy operates at high and permanent operational rates; spending on underwater protection becomes a structural and growing item in the defense budget; the selection of truly priority infrastructures highlighted by the hierarchy proposed in chapter 1, ceases to be an analytical exercise and becomes a daily operational necessity, because not everything is defensible at the same time. At the same time, in this future, Italy's centrality for the allies increases and the country could play a leadership role in the management of the underwater dimension.

Indicators of approach: appearance of autonomous long-range underwater systems in the export catalogues of second-tier manufacturers; first accidents attributed to non-state or proxy actors; increase in the frequency of "below threshold" accidents in the face of stable repair times; institutionalization of permanent allied operations to patrol the seabed in the Mediterranean.

6.3.3 Third scenario - The fragile quiet

Widespread proliferation, fragmented Euro-Atlantic system.

It is the worst future, and it must be described without indulging in dystopia precisely because its function is disciplining. The threat has democratized and the response has fragmented: autonomous systems of multiple origin and almost impossible attribution

operate on the bottom of the Mediterranean, low-cost sabotage has become an ordinary instrument of pressure, be it state, proxy or criminal, and each country protects what it can with what it has. The damage is transferred to the economy by insurance and logistical means: rising premiums on submarine assets, restoration delays measurable in months for those who do not have their own fleets, redundancy as a privilege of those who can afford it. The legal gray areas of the high seas, which Chapter 2 described as regulatory vulnerability, have become the standard operating space for hostile actors.

For Italy it is the scenario of forced and late renationalization. We would find ourselves forced to rebuild in an emergency, and therefore at the maximum cost, surveillance, repair and deterrence capacities that a twenty-five-year planning could have developed incrementally. Geography, which in cooperative scenarios is an income, is a condemnation here: the bottlenecks of Sicily and Otranto and the infrastructural density of the Italian seas offer hostile actors the maximum return per unit of effort. The hierarchization of infrastructures become triage.

Indicators of approximation: combination of the negative indicators of the two previous scenarios; appearance of serial sabotage not attributed in basins other than the Baltic; withdrawal or downsizing of private operators from Mediterranean routes judged not to be insurable; first cases of denial of infrastructure service explicitly used as a negotiating lever.

6.3.4 Fourth scenario - The disputed abyss

Contained proliferation, fragmented Euro-Atlantic system.

It is the deceptive future, and for this reason perhaps the most insidious. The threat has not democratized: the ability to act in depth remains concentrated in a few state hands. But the Euro-Atlantic construction has stalled and the protection of infrastructures has regressed to a mosaic of national initiatives, while the industrial function of laying and repairing has been concentrated almost entirely in non-European private operators and hyperscalers, which guarantee their systems levels of redundancy and restoration capacity precluded to public or minor infrastructures. Apparent security is high because deliberate accidents are rare; real security is low, because the few capable actors retain an intact and selective power of blackmail, exercisable at the moment of maximum leverage and the pre-positioning documented in chapter 3 suggests that the preparation for that moment would have taken place in silence, years before.

Italy, in this future, has outsourced without ever having decided to do so: national connectivity depends on the commercial planning of private entities that negotiate on an equal footing with states; repair capacity is bought on the market, with times and priorities dictated by others; the Navy maintains excellent skills but on an insufficient scale, and Law 9/2026 remains a legal architecture to which no means correspond. It is the scenario of dormant vulnerability: nothing happens, if everything happens together.

Indicators of rapprochement: non-renewal or phasing-out of dedicated NATO/EU formats; increasing share of new Mediterranean cable systems that are entirely private and without European participation; lengthening of average repair times for non-

hyperscaler infrastructures; decline of national investments in underwater capabilities downstream of years without major incidents.

6.4 What the scenarios teach: robust measures and contingency measures

The value of the exercise does not lie in narratives, but in what it allows us to distinguish. By subjecting the lines of response that emerged in the previous chapters to the test of the four futures, some measures are robust and necessary in all scenarios, while others remain contingent, the return of which depends on the future that will materialize.

Firstly, four lines of action are robust. The national capacity for surveillance and situational awareness of the seabed: it serves in the cooperative scenario as a contribution to the allied system, in the competitive scenario as a front-line tool, in the fragmented ones as a minimum safeguard of sovereignty and in any case feeds the attribution, a precondition for any response. Secondly, the full implementation of the architecture of Law 9/2026, which in three out of four scenarios makes the difference between a posture and an organizational chart. Thirdly, the protection of the industrial bottleneck installation and repair: it is the variable that most clearly separates sustainable futures from those suffered, and each of its declinations (participation in European programs, incentive for national capacity, priority agreements with operators) produces value in all quadrants. Fourthly, the hierarchization of infrastructures started in chapter 1: in benign scenarios it directs investments, in malicious ones it is the tool of triage.

On the other hand, they are contingent, and must therefore be accompanied by indicators rather than irreversible commitments: the sizing of the rapid response component (crucial in *submerged deterrence*, oversized in the *manned seabed*); the degree of reliance on collective mechanisms (rational in cohesive quadrants, risky in fragmented ones, where it must be balanced by minimum autonomous capacities); the bet on the cable hub as a growth vector, which yields a lot in ordered futures and increases exposure in disputed ones.

The last indication derives from this, of method rather than of merit: this chapter is not a point of arrival but a monitoring device. The indicators associated with each scenario should be reread periodically with the biennial review that appears proportionate to the speed of the size, updating the narratives when the signals accumulate, according to the logic of continuous monitoring and updating that the methodological literature considers an integral, and not accessory, part of the scenario analysis. The scenario that we consider most likely today will not arrive at 2050: the one that we will have been able, or not able, to recognize as it took shape will arrive.