



Technological security requires physically independent connections and autonomy in decision-making processes and strategic prioritisation



Satellites can maintain priority communications during a crisis, although their limited capacity means they must be treated as a backup



The physical independence of connections and the ability to maintain critical functions will increasingly influence the insurance, financing and valuation of digital assets

FROM CABLES TO SATELLITES: EUROPE'S BATTLE FOR DIGITAL RESILIENCE

Raúl VIÑAS ABADÍA

Afi

Submarine cables carry the vast majority of intercontinental internet traffic, yet the infrastructure itself remains physically exposed and increasingly caught up in geopolitical rivalry. Europe's position is especially fragile: beyond the cables' vulnerability, the continent depends heavily on non-European actors for the capacity, upkeep and satellite backup needed to keep networks running. Resilience therefore requires more than simply increasing the number of connections, as genuine diversity of suppliers, repair capacity and control over the alternatives available during a crisis are also crucial. Satellite links offer a stopgap for critical services during outages, but they lack the throughput and reliability to substitute for fiber at scale. As financial institutions and investors begin factoring physical connectivity into how they price risk and identify critical assets, submarine cable infrastructure is poised to matter as much economically as it already does strategically.

Introduction

European digital sovereignty rests on vulnerable physical infrastructure and, to a large extent, on foreign providers who supply capacity, maintenance and satellite backup. This combination turns connectivity into a matter of strategic control, because increasing the number of connections does not guarantee operational continuity if Europe lacks the capacity to reroute traffic and restore service during a crisis.

Many applications that European users perceive as global are delivered from data centers located within Europe, even when the provider is American. Major operators replicate data and critical workloads across multiple regions to reduce exposure to physical failures. This redundancy reduces the impact of isolated failures but

The European risk assessment carried out by the European Commission for 2025 estimates that U.S. hyperscalers account for around 90% of capacity between the United States and Europe and forecasts that their influence will continue to grow in other regions

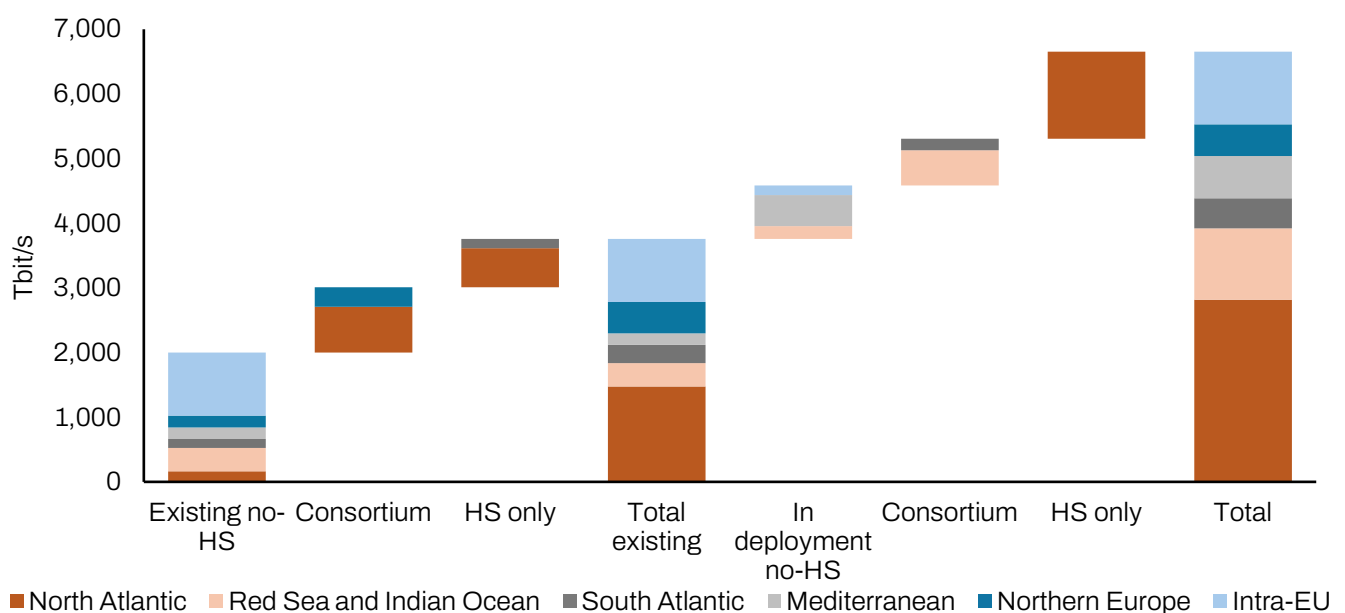
does not eliminate dependence on intercontinental routes or on their operational control. Submarine cables become critical when traffic crosses oceans, including synchronization between data centers, access to copies hosted outside Europe, international financial transactions, cybersecurity, telemetry, inter-cloud traffic and global business communications.

Over 99 % of intercontinental data traffic that crosses oceans travels via submarine cables, which are essential for the expansion of artificial intelligence, digital financial services and cybersecurity. [Their physical exposure brings forth a ‘grey area’ risk, as deliberate damage can be concealed amongst the approximately 200 annual faults in the global network, 80% of which are linked to fishing or anchoring.](#)¹ Incidents in the Baltic Sea in recent years have reinforced the perception that security depends on maintaining the ability to respond when a route ceases to function.

European connectivity, external control

U.S. hyperscalers have transformed the submarine infrastructure by funding the deployment of cables that directly connect their data centers and platforms. [The European risk assessment carried out by the European Commission for 2025 estimates that these companies account for around 90% of capacity between the United States and Europe and forecasts that their influence will continue to grow in other regions.](#)² This private investment makes it possible to expand capacity quickly and follows a clear operational rationale: hyperscalers connect their own data centers to reduce latency, ensure availability and maintain greater control over their services. Europe’s vulnerability emerges when intercontinental capacity, cloud infrastructure, traffic prioritization and part of its business continuity options depend on a highly concentrated corporate ecosystem dominated by U.S. companies.

Figure 1 - Submarine cable capacity connected to the EU by region and hyperscaler (HS) participation, 2025

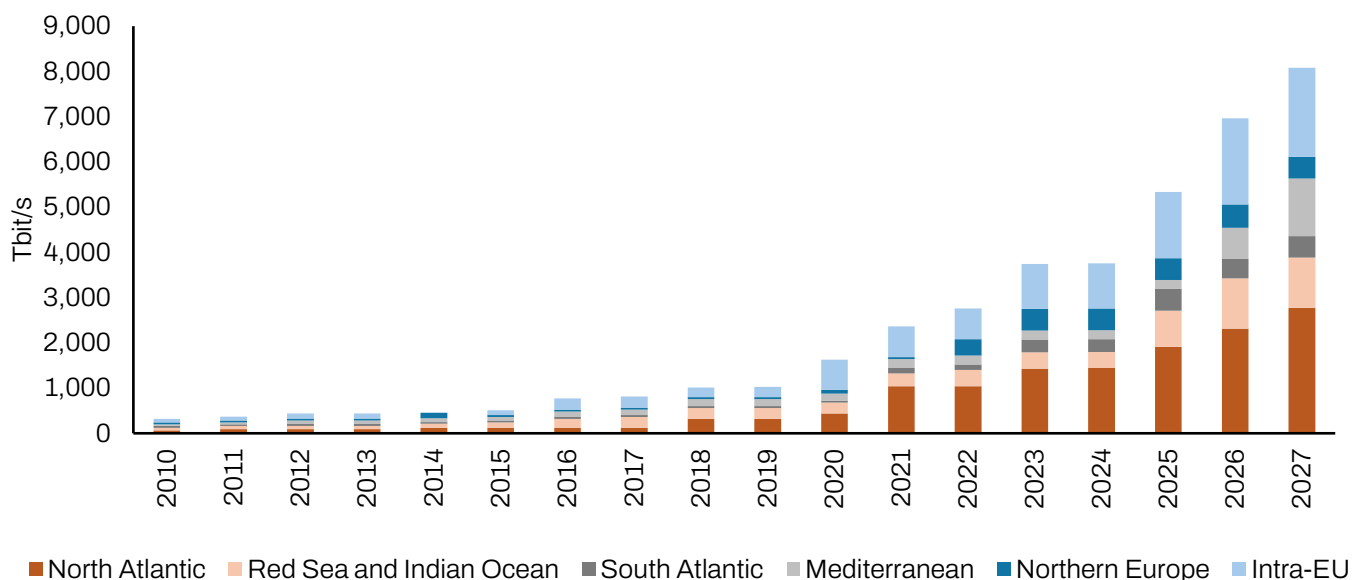


Sources: Authors' own elaborations based on European Commission (2025), Security and Resilience of EU Submarine Cable Infrastructures – Mapping, Risk Assessments, Stress Tests.

For Europe, this concentration primarily affects decision-making autonomy and the substitutability of critical capacities during a crisis. In the event of a serious disruption, the EU could find itself reliant on external interests to restore data traffic or to prioritize between incidents according to its operational needs. Consequently, the diversification of the European network should not be assessed by the number of cables, but rather by the concentration of suppliers, maintenance services or geopolitical alignments.

Chinese companies have less direct influence over transatlantic capacity and are less integrated into the European digital ecosystem, but they have gained a significant presence in the manufacturing and deployment of submarine systems and in projects in third countries that are key to the EU. Consequently, the European response is beginning to shift towards industrial policy. [In late 2024, France acquired 80% of Alcatel Submarine Networks, one of the few companies in the world capable of designing, installing and maintaining complete submarine systems, which had already deployed more than 750,000 kilometers of cable.](#)³ The acquisition does not eliminate Europe's dependence, but it preserves the industrial capacity to design, lay and repair submarine cable systems without relying entirely on external suppliers.

Figure 2 - Capacity of submarine cables landing in at least one EU Member State (2010-2027)



Source: Analysys Mason.

Restoring service before the disruption escalates

[Data from the International Telecommunication Union \(ITU\) shows that the global average time to commence a repair rose from less than 20 days in 2012 to more than 50 in 2024, despite the number of repairs and available vessels remaining relatively stable.](#)⁴ Permits and operational restrictions account for a significant part of this deterioration. Differences between regions are considerable. For example, the United Kingdom begins repairs within an average of around eight days because some maritime, environmental and coastal access permits are processed before

an incident occurs. In these cases, delays depend not only on the availability of a repair vessel, but also on whether it can operate legally and quickly at the site of the fault. Greater political attention to this infrastructure should help to extend such procedures and reduce some of the administrative delays, although there will continue to be constraints that are more difficult to address, such as the availability of specialized vessels, sea conditions or the distance to the point of failure.

Europe is in a comparatively favorable position in terms of vessel availability. The Commission's assessment notes that between 2022 and 2024, only around 2–3% of European incidents experienced delays because the required vessel was engaged in another repair. This advantage may be eroded if simultaneous outages increase and demand on a highly specialized fleet also rises. A deliberate campaign could seek precisely such saturation and turn sufficient capacity under normal conditions into a bottleneck.

[The Commission has set aside €347 million in 2026 to strengthen cable security, with funding for strategic projects, monitoring and repair modules deployable from European ports.](#)⁵ The first phase prioritizes the Baltic Sea and plans to extend this capacity to the Mediterranean and the Atlantic. This shift in focus is significant because it rightly shifts part of the response from emergency management towards pre-incident preparedness.

Low Earth Orbit (LEO) constellations can maintain essential connectivity during an emergency, but they lack the capacity to handle the volume carried by submarine cables

Satellites buy time; fiber carries volume

Low Earth Orbit (LEO) constellations can maintain essential connectivity during an emergency, but they lack the capacity to handle the volume carried by submarine cables. The aggregate capacity of a satellite network is much lower than that of large fiber-optic systems and, furthermore, must be shared amongst widely dispersed users and territories. Furthermore, although LEO satellites have significantly reduced latency, their performance deteriorates in the face of variations in congestion, coverage and changes in inter-satellite links. Finally, satellites still require ground-based infrastructure to connect traffic to data centers and local networks, meaning they do not eliminate physical points of failure. If several high-capacity cables were to fail simultaneously, the orbital network could sustain priority functions, but it would not be able to absorb the lost traffic.

The economic value of satellite backup will be greatest for those services where a brief disruption could have disproportionate effects. In the financial sector, keeping certain payment systems, critical communications or access to remote infrastructure operational may be sufficient to mitigate part of the impact whilst submarine connectivity is restored. This makes satellite constellations a layer of selective continuity, the importance of which will grow as reliance on digital services increases and tolerance for prolonged disruptions decreases.

This new layer of resilience introduces, however, another strategic concentration. If a large proportion of available orbital capacity depends on a few private constellations such as Starlink, technological diversification may still rely on a small

number of operators and jurisdictions. [In fact, SpaceX used the Ukrainian military's reliance on its Starlink connections to disable military operations in accordance with the company's internal criteria in 2022.⁶ Europe is seeking to reduce this reliance through IRIS²ⁱ, a project that has gained momentum in 2026 with the start of its large-scale deployment, but its first services will not be available until the end of the decade.⁷](#)

From connectivity to financial risk

[DORAⁱⁱ requires banks, insurers and other European financial institutions to identify critical technological dependencies, assess concentrations in third parties and prepare continuity and recovery mechanisms.⁸ It is therefore important to bear in mind that a deterioration in connectivity to data centers, payment systems or market infrastructure may necessitate the use of alternative capacity and delay operations. It can also have financial consequences without causing a complete disruption, including slower payments, delays in trade reconciliation, reduced access to market data, difficulties meeting margin calls or problems with cloud-hosted functions. In payment systems, a disruption that causes a backlog of pending orders increases pressure on settlement and intraday liquidity once the service is restored. \[The ECB has also warned that a well-capitalized institution may face serious problems if it loses critical functions during an operational shock.⁹\]\(#\)](#)

The valuation of digital assets will incorporate connectivity risks as technological concentration and geopolitical exposure increase

The risk profile of a data center can vary significantly depending on the physical independence of its connections, pre-arranged access to repair services and the backup capacity available to maintain critical functions. As these differences become more visible, they will also influence insurance costs, financing conditions and investor requirements. An asset that depends on concentrated routes, external providers that are difficult to replace or uncertain repair times will have a different risk profile from one with alternatives secured in advance and greater clarity over its physical points of failure. This development would be consistent with the emphasis that DORA and banking resilience frameworks already place on critical dependencies and continuity during severe disruptions.

Over the next five years, supervisors and insurers will demand more information on the physical routing of connections and the time required to restore them. The change will become apparent when resilience exercises begin to distinguish between genuinely independent routes and links that share vulnerable corridors. Contracts will likely progressively incorporate reserved repair capacity and satellite backup for priority functions. By the middle of the next decade, assets unable to demonstrate these safeguards could face higher premiums and less favorable financing terms. The decisive indicator for Europe will be the speed with which investments in repair modules and IRIS² deliver available capacity during a crisis. If infrastructure expands whilst operational control remains centralized, autonomy will advance far less than the capacity figures suggest. **FI**

i. EU Satellite Resilience, Interconnectivity and Security Infrastructure.

ii. Digital Operational Resilience Act, the EU's Digital Operational Resilience Regulation.

References

1. International Telecommunication Union (ITU) (2026). International Advisory Body on Submarine Cable Resilience – Report of the Working Groups 2026. <https://www.itu.int/hub/publication/s-iab-wg-2026/>
2. European Commission, Submarine Cable Infrastructures Expert Group (2025). Security and Resilience of EU Submarine Cable Infrastructures – Mapping, Risk Assessments, Stress Tests. <https://digital-strategy.ec.europa.eu/en/library/report-security-and-resilience-eu-submarine-cable-infrastructures>
3. Nokia (2025). Nokia completes its sale of its leading submarine networks business, ASN (Alcatel Submarine Networks), to the French State. <https://www.nokia.com/newsroom/nokia-completes-its-sale-of-leading-submarine-networks-business-asn-alcatel-submarine-networks-to-the-french-state/>
4. International Telecommunication Union (ITU) (2026). International Advisory Body on Submarine Cable Resilience – Report of the Working Groups 2026. <https://www.itu.int/hub/publication/s-iab-wg-2026/>
5. European Commission (2026). Commission boosts submarine cable security with a €347 million investment and a new toolkit. <https://digital-strategy.ec.europa.eu/en/news/commission-increases-submarine-cable-security-eu347-million-investment-and-new-toolbox>
6. Associated Press (2023). Elon Musk's refusal to have Starlink support Ukraine's attack in Crimea raises questions for the Pentagon. <https://apnews.com/article/fde93d9a69d7dbd1326022ecfdb53c2>
7. European Space Agency (ESA) (2026). IRIS² reinforced and accelerated as implementation advances. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/IRIS2_reinforced_and_accelerated_as_implementation_advances
8. European Union (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act, DORA). <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
9. European Central Bank (2026). Elderson, F., 'Strengthening operational resilience for the age of AI'. Keynote speech at the Goldman Sachs European Financials Conference 2026, Zurich, 3 June 2026. <https://www.ecb.europa.eu/press/key/date/2026/html/ecb.sp260603~5b8e67f237.en.html>