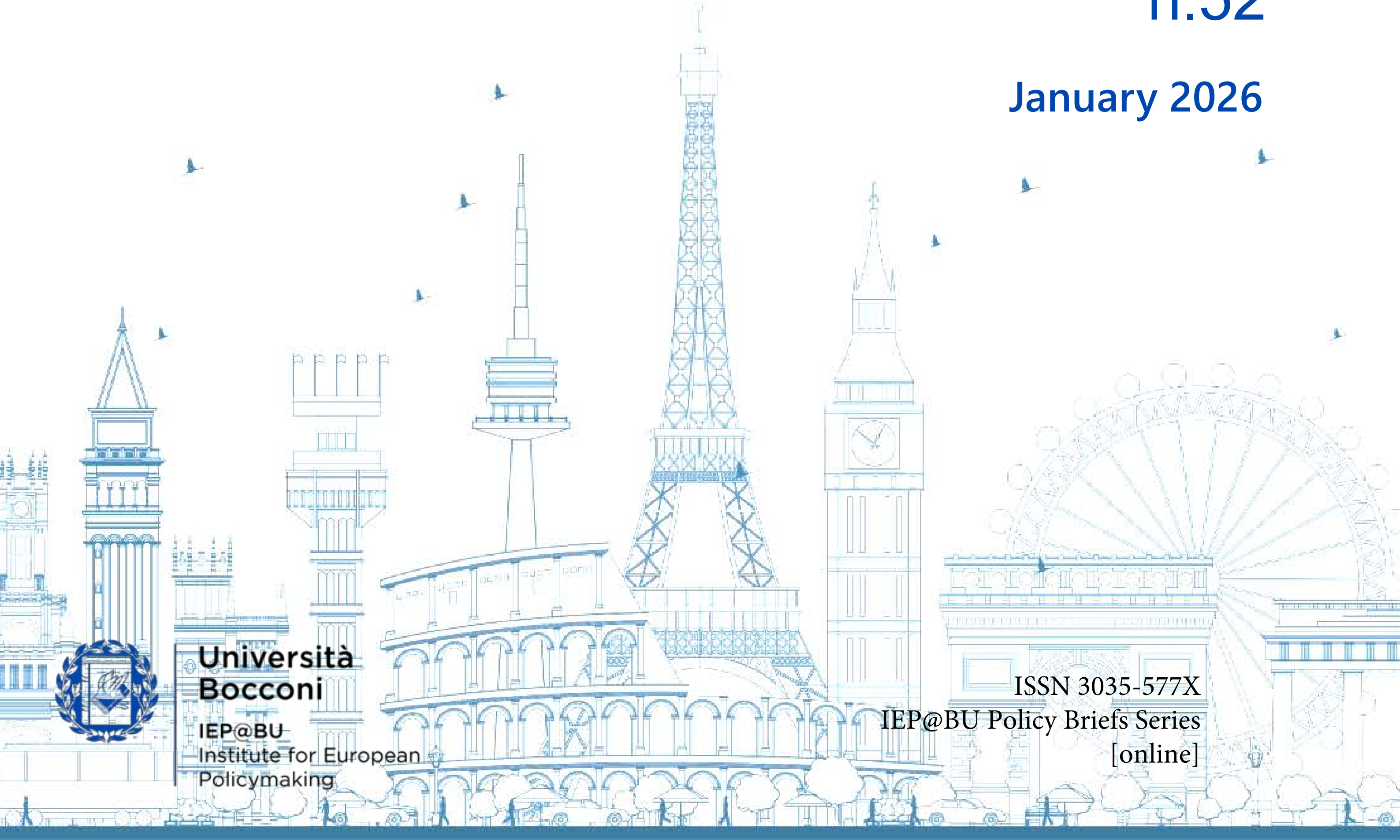
PER ASPERA AD ASTRA: UNDERSEA CABLES, SATELLITES FOR TELECOMMUNICATIONS AND THE EUROPEAN STRATEGIC AUTONOMY

Giovanni **Cabroni**, Andrea **Gilli**

IEP@BU Policy Brief
n.52

January 2026



Università Bocconi
IEP@BU
Institute for European Policymaking

ISSN 3035-577X
IEP@BU Policy Briefs Series
[online]

IEP@BU does not express opinions of its own. The opinions expressed in this publication are those of the authors. Any errors or omissions are the responsibility of the authors.

Per aspera ad astra: undersea cables, satellites for telecommunications and the European strategic autonomy[1]

Giovanni Cabroni & Andrea Gilli[2]

[1] The author would like to thank Thi Phuong Thao Pham, Giovanni Tricco, Daniel Gros, Stefano Feltri, Clemence Poirier, Carlo Altomonte, Simonetta Di Pippo, Alessio Terzi, Antonio Deruda and Francesco Nicoli for the extensive comments.

[2] Giovanni Cabroni is Analyst at Novaspace and a former Research Assistant at the Institute of European Policy-Making at Bocconi University. Andrea Gilli is Associate Fellow at the Institute of European Policy-Making, Lecturer at the University of St Andrews, Expert Mentor at NATO Diana, Non-Resident Senior Fellow at the NATO Defense College and Senior Advisor at the Office of the Undersecretary of State for Defense in Italy. The opinions expressed are the authors' only.

Executive summary

Digital technologies have become the core enabler of social interactions, economic transactions and security dynamics around the world. Europe currently lags behind in core digital or digital-enabling technologies, from rare earths production to semiconductors design and manufacturing capabilities to big tech enterprise software.

Europe, however, is also increasingly vulnerable when it comes to connectivity, the arteries underlying digitalization. In particular, its undersea cables transporting data across the Atlantic Ocean, the Northern, Baltic and Mediterranean Seas are increasingly vulnerable to Russian sabotage.

In outer space, Europe is either seeing its satellites becoming more vulnerable to a wide spectrum of adversarial capabilities (from cyberattacks to jamming) or is becoming more dependent on foreign solutions, like Elon Musk's Starlink low-Earth orbit (LEO) communication satellites constellation.

Undersea cables and communication satellites are generally treated separately. In this Policy Brief, we consider them together, looking at how these two infrastructures can support each other for the purpose of strengthening Europe's sovereignty, resilience and security. In our analysis, we first identify three key trends.

Undersea cables will continue to carry most intercontinental data across the Atlantic – at least for the foreseeable future. Protecting undersea cables is, however, expensive and subjected to diminishing marginal returns given the size of the areas and the multiple types of threats they face.

Finally, LEO communication satellite constellations will experience a massive growth of their capacity; however, given the overall increase in data transfer, LEO communication will remain an important, but minor, part of the data transmission infrastructure.

Second, we derive a set of considerations. Given their large domestic contracts, supply- and demand-side economies of scale they enjoy, and the technological advantage they possess (from launchers to satellite manufacturing), U.S. companies like Starlink or Amazon Leo (formerly Project Kuiper) are likely to maintain a quasi-monopolistic position for the near future in LEO communication satellites.

Thus, European LEO projects – more prominently, the EU flagship project IRIS^{2} (Infrastructure for Resilience, Interconnectivity and Security by Satellite) – have zero chances of successfully competing commercially. For, IRIS^{2} should be transitioned to strategic tools for governments, militaries, and crisis situations.

Even if the capacity is limited compared with US and Chinese competitors, it is more than enough to keep essential national functions online.

Along with continuing monitoring and protection of undersea cables, the EU should also invest in hybrid cable-satellite system architecture that can switch automatically when cables fail, following progress achieved by NATO-led HEIST project (Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunications).

These steps would make Europe far more resilient, improving security, strategic autonomy as well innovation and cooperation among EU Member states.

Introduction

Digital data, much like electricity in the 20th century, is the defining feature and critical enabler of the world economy today.

Every industry – from research to logistics, finance to defense– relies on secure digital connections, powered by largely invisible infrastructures: undersea cables, satellites, data centers, and cloud networks.

These systems sustain the continuous global flow of information, capital, and ideas, forming the backbone of modern interdependence.

Paradoxically, the strategic importance of these infrastructures is matched by their fragility as they are mostly unseen, largely unprotected, and increasingly vulnerable. Submarine cables, in particular, transmit 95% of all data worldwide and face routine threats from accidents and natural events, as well as intentional adversarial disruption.[3]

Of these data, only a minimal fraction is represented by military, government and other critical and high value data – e.g. financial transaction data – which, however, are critical for the economy.

As hostile tactics evolve, adversaries exploit the opacity of the seabed and the congestion of orbital space to turn the interdependence of physical infrastructures into a frontline of geopolitical competition.

Europe’s position is particularly fragile in this respect. The continent’s digital lifelines run through foreign-owned networks; its cables cross crowded, shallow seas adjacent to revisionist powers; and its space capabilities lag those of the United States and China.

Recent disruptions – including suspected sabotage in the Baltic and North Seas – demonstrate the ease with which European connectivity can be compromised.

In response, NATO launched Operation Baltic Sentry in January 2025, marking the first collective effort to monitor and defend seabed infrastructure. Yet, defending these assets is costly, complex, demands constant vigilance and overall is subjected to decreasing marginal returns.

At the same time, the rise of low-earth orbit (LEO) satellite constellations such as Starlink and Amazon Leo and the growing dominance of SpaceX and – more recently – Blue Origin in the space launch business with their reusable rockets, have exposed Europe’s delay and dependency, which acquire particular salience in a time of transatlantic turbulence.

In this Policy Brief, we approach these issues jointly: rather than discussing cables and satellites in silos, we look at them together to identify possible options for Europe.

We proceed in four steps. First, after a general introduction to subsea cables for communications, we focus more deeply on the European network, analyzing its scale, vulnerabilities, and critical choke points.

Second, we assess Europe’s satellite ecosystem, highlighting capacity constraints and technological

[3] Telegeography (2025)

dependencies.

Third, we show how these two systems, in space and under the sea, are interdependent, from technical, geopolitical and security perspectives. Finally, we advance our policy recommendations.

2. Submarine cables: the backbone of global and European connectivity

Submarine communication cables (SCCs) are the silent arteries of Europe's digital economy. They carry the overwhelming majority of global (i.e., intercontinental) data traffic, underpin cloud services and AI, sustain financial markets, and connect Europe to its neighbours and strategic partners.

Although satellites are indispensable for resilience and emergency communications, SCCs remain the core infrastructure enabling the world's data transmission – Europe included.

SCCs are also critical from a military perspective: US and EU navies have begun transforming parts of the global fiber-optic undersea cable network into vast underwater sensing systems through Distributed Acoustic Sensing (DAS).

This technology sends laser pulses along the SCCs to detect vibrations from submarines and ships, effectively converting communication infrastructure into passive sonar. As nations test and adopt DAS, SCCs are becoming even more strategic – and consequently more attractive targets for hybrid warfare.[4]

This chapter examines SCCs through three lenses: Europe's strategic weaknesses, the vulnerabilities and costs associated with cable disruptions – including comparisons with other undersea critical infrastructures – and the major European chokepoints from a cable-centric perspective.

2.1 Strategic Weaknesses

Stretching almost 1.4 million kilometres across the world's oceans, SCCs carry the majority of the global data traffic. With the rise of fiber-optic cables in the late 1980s and the growth of the Internet, SCCs became the most used way to transmit data, surpassing satellites.

Indeed, t[5]￼

Currently, there are nearly 600 active and planned SCCs worldwide and Europe is uniquely exposed, with nearly 200 cables connected and an extensive network of 300 landing stations[6].

[4] https://interestingengineering.com/military/us-eu-navies-submarine-hunting-sonars

[5] Sources: https://en.wikipedia.org/wiki/Dunant_%28submarine_communications_cable%29; https://en.wikipedia.org/wiki/Grace_Hopper_% 8submarine_communications_cable%29 ; https://committees.parliament.uk/writtenevidence/138729/default; https:// ; www.capacitymedia.com/article/2d0tkm9h4o2jcptw4w740/feature/9-of-europes-most-important-submarine-cable-projects

The total submarine cable capacity connecting the EU Member States between themselves and to outside countries has increased from 318 Tbit/s in 2010 to 3,755 Tbit/s today. SCCs are becoming increasingly critical, and for Europe three main weaknesses persist:

- **Geography of cables**: European seas are shallow, busy, and crowded with subsea cables and other undersea critical infrastructures. This density provides connectivity but also a high surface of exposure. Furthermore, the 33 newest cables provide 74% of the total capacity currently provided by submarine cables landing in at least one EU Member State.[6] In contrast, the 89 oldest cables represent only 2% of the total current capacity of submarine cables landing in at least one EU country.[6]
- **Ownership and dependency**: a growing portion of European-facing transatlantic systems are financed and operated by US big tech hyperscalers. These firms account for 71% of all used international capacity in 2024, up from 10% in 2014.[6]

The strategic dependency is amplified by Europe's slow growth in data centers and data processing, especially now with the rise of AI applications. Furthermore, SCCs can be leased by multiple operators.

It means that the same infrastructure simultaneously carries high-value assets such as medical records, governmental communications, or financial transactions, alongside commercial data streams like video and entertainment services.

- **Protection challenges and diminishing returns.** Monitoring thousands of kilometres of seabed is expensive and technically complex. Naval patrols, seabed sensors, satellite images and data, and autonomous vehicles provide improvements – but never full coverage.[7][8]

Each additional layer of protection costs more and yields less, leaving adversaries ample room to operate in the "gaps" of surveillance.

NATO Operation Baltic Sentry, even if essential for signalling presence and ensuring security and

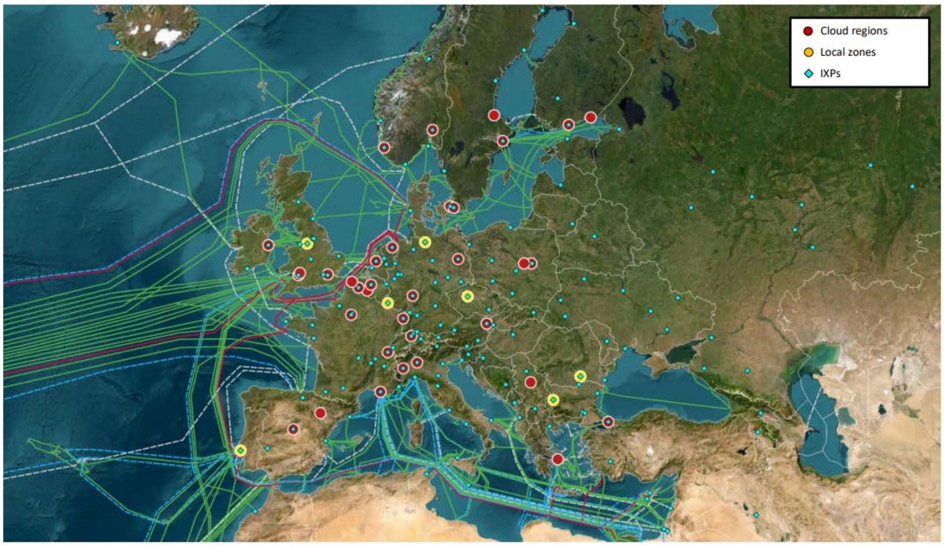
[6] Submarine Cables Expert Group - Mapping risks stress tests, EU Commission (2025)

[7] (i) **EO satellites** provide wide-area monitoring of cable corridors, detecting vessel tracks, anchor drag, turbidity plumes, or other surface anomalies that may indicate damage or interference. Synthetic-aperture radar (SAR) in particular allows all-weather, day/night surveillance along SCC routes. (ii) **GNSS satellites** support precise positioning for cable-laying, inspection ROVs, and repair vessels, while also enabling AIS-GNSS integration to track ship behaviour around sensitive areas. GNSS timing signals are essential for synchronising distributed sensing systems along fibre networks. (iii) **IoT/IoUT satellites** allow sparse seabed and near-seabed sensors, acoustic nodes, and unmanned surface/underwater vehicles to transmit data from remote locations. This enables continuous detection of strain, temperature, vibration or intrusion events along SCCs, providing real-time alerts even far from terrestrial coverage.

[8] Non-satellite CUI protection relies mainly on **seabed and near-seabed sensing** – including distributed acoustic sensing (DAS) on fibre pairs, hydrophones, pressure and vibration sensors, and smart repeaters capable of detecting anchor drag or tampering. **Uncrewed systems** such as AUVs and ROVs perform inspection, mapping, and rapid damage verification, while **USVs and maritime drones** provide persistent surface patrols along cable corridors. In shallow waters, **cable burial, armouring, and exclusion zones** remain primary defences, complemented by AIS-based anomaly detection and coastal radar. These systems create a localised but high-resolution monitoring layer that complements the broad-area awareness provided by satellites.

surveillance in the Baltic Sea, is a perfect example of these diminishing returns.

Figure 1: Map of European cables, cloud regions and IXPs in 2025[9]



Source: Submarine Cables Expert Group - Mapping risks stress tests, EU Commission (2025)

2.2 Vulnerabilities and Disruption Costs: a comparison with other undersea infrastructures

SCCs are exposed to three categories of threats: accidental damage (by far the most common), natural events, and deliberate interference.

Accidents typically involve fishing gear or anchors dragged across the shallow seabed and they are the most common cause of disruption. Natural hazards such as underwater landslides, seismic activity, and storms can brake cables.

Deliberate disruption – covert sabotage or grey-zone interference – has grown sharply in recent years, especially in the Baltic and the High North approaches (Figure 2 and Appendix A). Meanwhile, repair is slow and costly.

The global fleet of cable-laying and repair vessels numbers fewer than 100[10] and the direct repair cost of a single break usually ranges from €3–8 million; but the indirect economic losses are far more

[9] **Cloud regions** are big data-centre hubs where cloud providers store and process large amounts of data. **Local zones** are smaller, nearby extensions that bring cloud computing closer to users for lower latency. **IXPs** (Internet Exchange Points) are physical locations where different internet networks connect and exchange traffic directly.
[10] Report on Security and Resilience of EU Submarine Cable Infrastructures, EU Commission (2025)

severe.[11] A single disrupted SCC can trigger losses of up to $50 million per day.[12]

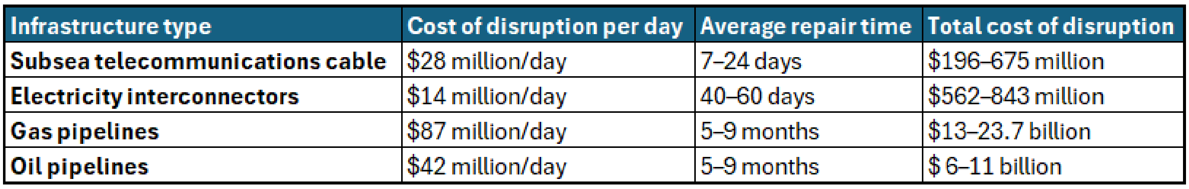
Other estimates, especially for advanced economies, are more conservative, with $28 million per day and an estimated range time for repairing of 7-24 days.[13] By multiplying those numbers, the total amount of economic loss for an SCC could range from $196 to $675 million.

In advanced economies with greater redundancy the economic shock is less dramatic but still significant.

Compared to other undersea critical infrastructures (UCIs), SCCs are paradoxical (Table 1): energy pipelines and power cables generate higher per-event economic losses, but SCCs face far more frequent disruptions and are harder to secure across their full length. Operators therefore prioritize protection for:

- new, high-capacity cables with limited redundancy;
- landing stations, which are easier to defend physically and connect more cables in the same point;
- vulnerable shallow-water segments where sabotage or accidents are most likely, not only for SCCs but also for other UCIs.

Table 1: Economic losses comparison of different UCIs



Infrastructure type	Cost of disruption per day	Average repair time	Total cost of disruption
Subsea telecommunications cable	$28 million/day	7–24 days	$196–675 million
Electricity interconnectors	$14 million/day	40–60 days	$562–843 million
Gas pipelines	$87 million/day	5–9 months	$13–23.7 billion
Oil pipelines	$42 million/day	5–9 months	$ 6–11 billion

Source: adapted from Evolving threats to critical undersea infrastructure: Implications for European security and resilience, Rand (2025)

The strategic implication is clear: adversaries can inflict outsized economic and political damage with limited resources.

2.3 European Critical Chokepoints: A Cable's Perspective

Europe's cable geography can be thought of as a network of different critical gateways. Each presents distinct vulnerabilities, forms of redundancy, and strategic stakes.

[11] Evolving threats to critical undersea infrastructure: Implications for European security and resilience, Rand (2025)

[12] https://www.unclosdebate.org/evidence/329/empirically-disruption-undersea-cables-cost-millions-dollars-hour-lost-revenue The amount is 36 million USD and it's from 2013, so in today's money it would be 36*1,39 = 50,04 Source: https://www.in2013dollars.com/us/inflation/2013?amount=1

[13] https://www.rand.org/pubs/perspectives/PEA3800-1.html

- **Atlantic Gateway:** the Atlantic is Europe's most important digital artery. Nearly all EU–North America data flows cross a small set of landing points in Ireland, the UK, France, and Portugal. High value financial data, streaming and video transmission and AI applications are possible thanks mostly to the cables in this area. Furthermore, different European islands and archipelagos are located here. Ireland, in particular, is an island nation, which relies on digital and financial data for its rich service-based economy.
- **North Sea**: the North Sea hosts one of Europe's densest SCCs and energy corridors, linking the UK, Norway, Denmark, Germany and the Netherlands. Shallow waters and heavy maritime traffic make accidental damage frequent, while the coexistence of offshore wind farms, pipelines and power cables complicates monitoring. Recent disruptions near Shetland illustrate the fragility of the region (Figure 2, Appendix A). Although redundancy is relatively high, the concentration of multiple undersea critical infrastructures creates systemic risk.
- **Baltic Sea and Baltic States:** the Baltic has emerged as Europe's grey-zone hotspot, with the sabotage of the North Stream. The most recent suspected sabotage incidents regarding SCCs – C-Lion1, EE-S1, BCS Interlink, FEC-1/FEC-2 – occurred here (Figure 2, Appendix A), often involving vessels departing Russian ports.

  Moreover, Estonia, Latvia and Lithuania are effectively a "digital peninsula": connected to continental Europe mainly through a narrow Polish land corridor and a handful of fragile subsea links. Redundancy exists, but vulnerabilities are structural. Any coordinated disruption could rapidly isolate the region.

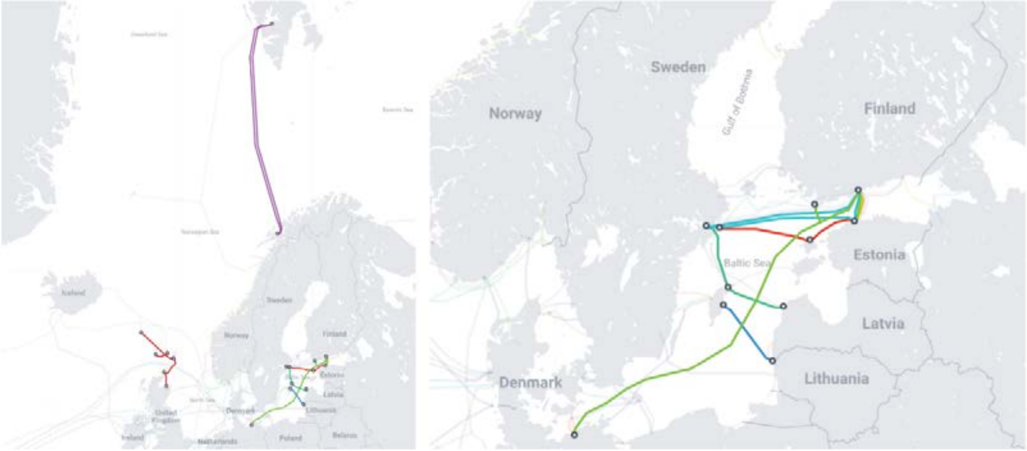
- **High North and Arctic Corridor:** melting ice is enabling the development of new Arctic cable routes but also exposing them to greater maritime activity and environmental volatility. The Svalbard Undersea Cable System – supporting the world's most important polar ground station – has already faced suspicious breaks (Figure 4, Appendix A). Future projects such as Far North Fiber and Polar Connect promise diversification but will operate in an inherently fragile environment marked by ice scouring, remoteness, and geopolitical contestation.
- **Mediterranean and Southern Routes:** the Mediterranean connects Europe with North Africa, Asia, and key island territories such as Cyprus and Malta, which are island States and rely on digital connectivity for their economies.

Redundancy is uneven: Southern Europe enjoys multiple routes, while North African links remain limited, and some island countries depend on just one or two cables. The region's chokepoints – Strait of Sicily, Eastern Mediterranean routes, and Levantine basins – combine high geopolitical tension with limited repair capacity. Lessons from the 2024 West Africa outages highlight the risks for regions lacking sufficient backup capacity.[14]

[14] In March 2024, an underwater landslide off Côte d'Ivoire severed four major cables, cutting or slowing internet across 16 West and Central African countries. With almost no redundancy, traffic could not be rerouted, causing widespread service collapse and large economic losses until repairs were completed. Source: https://carnegieendowment.org/research/2025/03/beneath-the-waves-addressing-vulnerabilities-in-africas-undersea-digital-infrastructure

- **Other territories and assets overseas:** Europe's digital perimeter includes outermost regions and overseas territories across the Atlantic, Caribbean, and Indian Ocean. Many – such as the Azores, Madeira, Canary Islands, Réunion, Mayotte, Martinique, Guadeloupe, French Guiana, Saint-Martin – depend on only one or a few SCCs, creating high isolation risk during faults or sabotage. Strengthening and guarantying their redundancy is essential.

Figure 2: maps showing the location of disrupted cables in Northern Europe and the Baltic (2021-2025). On the right, a deep focus on the Baltic Sea (Please refer to appendix A for a more in-depth analysis)



Source: [Telegeography Undersea Cables Map, 2025.]

Finally, the strategic role of cables was acknowledged by EU. Through the EU Connecting European Facility (CEF) Digital, more than €420 million has been allocated to 51 connectivity projects between 2021 and 2024, including both SCCs and land cables projects. An additional €540 million has been earmarked for 2025–2027, bringing total EU spending on digital backbones close to €1 billion.[15]

The critical role of cables is also signalled by the Cable Security Action Plan (2025) and the recent reports in late October of this year on cables security, published by the European Commission.

3. Satellites: The Orbital Dimension of Connectivity

If SCCs are the arteries of digital life, satellites are its capillaries – connecting remote regions, enabling navigation and surveillance, and delivering secure communications. Satellites also offer, albeit with limited bandwidth, an alternative to cables in case of attack or cable disruption.

[15] https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables

Together, SCCs and satellites form the sea–space continuum essential to modern economies. This chapter explores the operating architecture of satellites and Europe's place in orbit.

3.1 Satellites for Telecommunication: from GEO to LEO

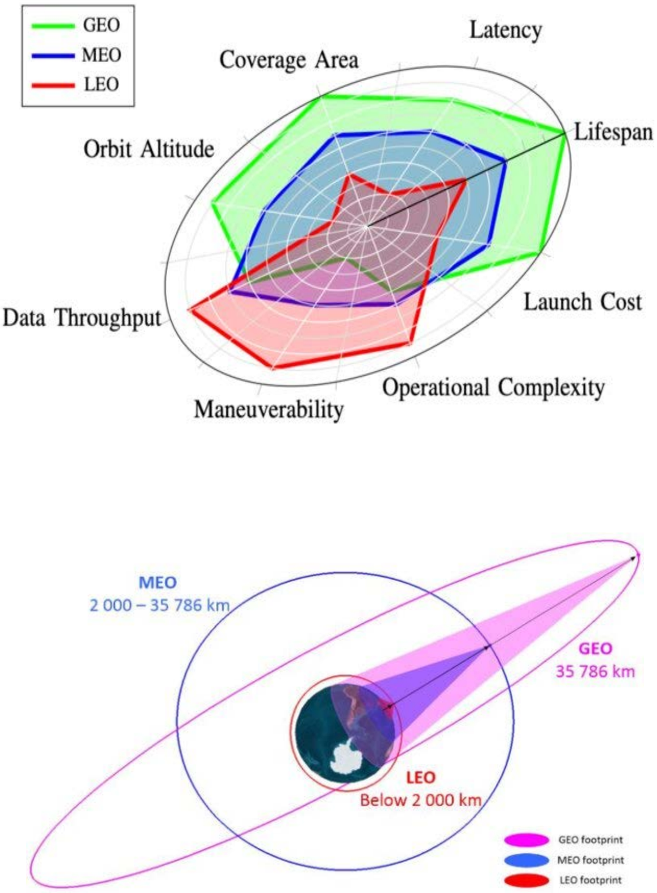
Satellites serve three main purposes: navigation, observation and communications. Navigation satellites like the U.S. GPS or the European Galileo enable geolocation.

Observation satellites, like the U.S. NOAA or the Italian COSMO Sky-med constellations permit to gather images from the orbits (for a plurality of activities, from weather to military). Communication satellites permit datalinks to connect two earth-based points. In this section, we focus only on communication satellites (Satcom).

Satellites can orbit the earth in different ways. For our analysis, which focuses on satellites for telecommunications, the relevant orbits are three: Low earth Orbit (LEO), Medium Earth Orbit (MEO) and Geostationary Orbit (GEO). Each of this orbit has different characteristics and trade-offs, summarized in the table below and in Figure 3.

Orbit	Altitude	Advantages	Disadvantages
LEO	160–2,000 km	Low latency (<50 ms), high data capacity, low launch cost, high manoeuvrability	Narrow coverage area (for a single satellite), high operational complexity, low lifespan (usually 5-7 years)
MEO	2,000–35,786 km	Wider coverage, moderate latency. In between LEO and GEO. Requiring fewer satellites than LEO, lower launch cost than GEO	Higher latency than LEO (usually between 100 and 200 ms) and less capacity
GEO	35,786 km	Fixed relative to Earth, very wide coverage, low operational complexity, high lifespan (usually 15-20 or even more years)	High latency (~600 ms) , low manoeuvrability, low capacity, high cost

Figure 3: illustrations showing LEO, MEO, GEO and the latency-coverage trade-off. On the right, a radial graph summarizing the advantages and disadvantages of the three orbits.



Source: Sustainable Satellite Communications in the 6G Era: A European View for Multi-Layer Systems and Space Safety Höyhtyä et al. (2022); LEO Satellite and RIS: Two Keys to Seamless Indoor and Outdoor Localization, Zheng et al. (2024)

Since the 1960s, GEO satellites have provided global coverage for broadcasting and government communications. Fixed above the equator, they blanket continents but face major limits, not only regarding latency but also data capacity.

While modern GEO satellites such as ViaSat-1, ViaSat-3, and EchoStar XVII can handle up to one terabit per second, most other GEO satellites deliver far less (1-12 Gbps, or 0.001-0.012 Tbps), and their aggregate capacity remains extremely low compared to LEO satellites.[16]

All GEO systems worldwide provide only about 7 Tbps of usable capacity, while LEO systems have nearly 50 Tbps of usable capacity (Figure 4). On the other hand, LEO and MEO constellations

[16] https://www.viasat.com/perspectives/corporate/2022/what-is-viasat3/

replace isolated satellites with coordinated constellations of smaller craft. Proximity to Earth means lower latency and scalable growth.

The logic of constellations replaces the logic of individual GEO satellites: capacity is no longer tied to one satellite's footprint but distributed across swarms of satellites, in constant motion and always able to connect with the receiving device or ground station on Earth.

Constellations and mega-constellations – defined as constellations with more than 1,000 satellites – are designed not only to increase capacity and cut launch costs but also to make life easier for satellite operators.

Their scale and built-in redundancy mean that when a few satellites stop working, replacements can be launched without disrupting the network's overall performance.

Overall, the model lowers development and operational costs while ensuring detailed global coverage, enabling new services. LEO satellites, thanks to the extreme low latency, could offer services such as gaming, 5G/6G communications, autonomous vehicle control, fast trading in every corner of the world.

Looking at the near future, over the next five years, total LEO and MEO capacity is expected to increase by more than 5 times, probably reaching over 300 Tbps after 2030 (Figure 4). Three dynamics underpin this growth:

- Payload scaling: the orbital data capacity of a single satellite has risen from single-digit Gbps in 2015 to up to 1 Tbps (1000 Gbps) in next-generation designs.

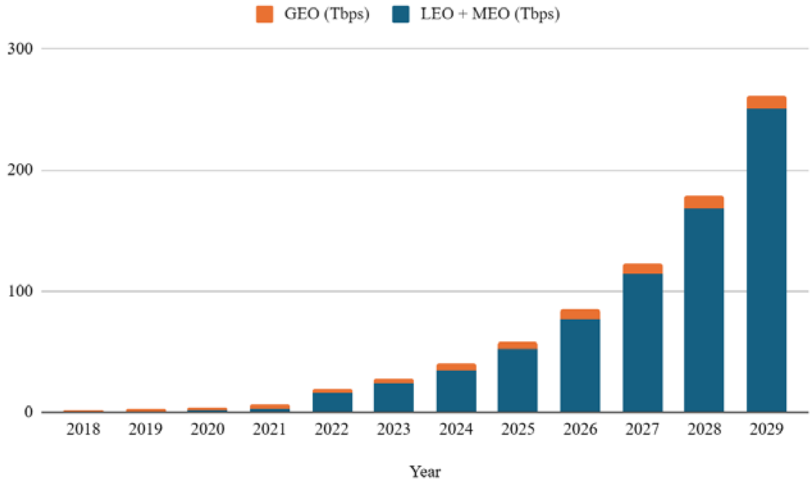
- Launch economics: the cost per kilogram to orbit, especially in LEO, has fallen by more than 90% since 2010, thanks to reusable rockets like Falcon 9 and soon the future Starship from SpaceX and an increasingly smaller size of satellites, enabling the deployment of thousands of satellites per year.[17]

- Network design and technology: new constellations are being equipped with laser links that enable satellites to communicate directly with each other and from different orbits, creating so-called "mesh" constellations. Furthermore, new technologies are enabling onboard processors, which can manage and process data directly in space. This will allow to have in-orbit AI and ML applications, making connectivity faster and more efficient, by predicting traffic demands, detecting anomalies, and rerouting data path.[18]

[17] Adilov, Nodir & Albertson, Nikolas & Alexander, Peter & Cunningham, Brendan. (2021). An Economic Analysis of Launch Cost Reductions for Low Earth Orbit Satellites.

[18] Tricco et Al., The protection of AI-based space systems from a data-driven governance perspective, Acta Astronautica, Volume 234, 2025, Pages 73-86, ISSN 0094-5765, https://doi.org/10.1016/j.actaastro.2025.04.063.

Figure 4: Current estimate and projections for total usable data capacity from GEO and Non-GEO satellites worldwide, 2018-2029



Source: interpolation of data from https://nova.space/press-release/satcom-providers-change-tactics-to-compete-with-ngso-led-capacity-growth/; https://apscc.or.kr/wp-content/uploads/2018-APSCC-Q4-web.pdf ; https://apscc.or.kr/wp-content/uploads/2018-APSCC-Q4-web.pdf ; https://ts2.tech/en/bandwidth-wars-the-high-stakes-battle-for-high-throughput-satellite-dominance-2025-2035

Following this trend, it is not possible to completely exclude that, in the really long term, satellites' capacity could be able to compete – at least partially – with SCCs'.

3.2 The future of satellite communications and the race for LEO orbit dominance: US vs China

More than 80% of LEO satellite data capacity belongs to the U.S. company SpaceX, with its LEO mega-constellation Starlink, the first in human history.

Launched in 2019, Elon Musk's constellation Starlink has, as of 14 June, 2025, launched 8,971 satellites. Of these, 7,782 remain in orbit and 7,759 are still operational, leaving around 1,212 that have re-entered or gone offline – roughly 13.5% of the total.[19]

In systems as dense as Starlink, with a planned constellation of 40,000 satellites by 2040, even the loss of dozens – or hundreds – of units barely dents functionality, since the constellation is engineered for resilience.

This scale enables Starlink to leverage network effects, where the value of its service increases with each additional satellite and user, creating a self-reinforcing cycle of adoption.

Starlink's competitive pricing, offering high-speed internet at accessible rates for both consumer markets, such as individual households in remote areas, and business clients, including enterprises

[19] Di Pippo S., *SPACE ECONOMY - II ED. L'arena Competitiva del Futuro*, Bocconi University Press, 2025

and governments, further solidifies its global appeal.[20]

Furthermore, this mega-constellation offers global broadband, which has not only commercial value but also military utility, as demonstrated directly on the battlefield: in Ukraine, Starlink enabled resilient military communications after the terrestrial infrastructure was destroyed by Russia.

Its rapid deployment, flexible coverage, and low latency turned satellite internet into an essential strategic asset.[21] Indeed, SpaceX is also working for the US Department of Defense to build Starshield, a secure satellite network for military applications, enhanced with anti-jamming systems.

Starlink, however, is not alone. In the competition of American multibillionaires to dominate outer space, Jeff Bezos' Amazon Leo (former Project Kuiper) entered the field in 2023, with a planned mega-constellation of over 3,000 satellites.[22] This LEO constellation will leverage the consolidated ground infrastructure of Amazon Web Services (AWS), with data centers and massive SCCs projects, to deliver cloud connectivity and data processing for global enterprises.

This will reinforce U.S. leadership in commercial and industrial applications and will allow Amazon to compete with Starlink, even with a smaller fleet.[19]

China is also accelerating. Its planned Guowang mega-constellation – with an expected size of 13,000 satellites – is explicitly designed as a national champion, with state ownership and military integration.

Furthermore, Beijing announced two other projects: the commercial mega-constellation Qianfan – with a planned size of 15,000 satellites – and the military mega-constellation Honghu-3, still in an R&D phase, with up to 10,000 satellites.[23]

These huge projects remain in early stages, but they show the ambitions of China, which, unlike Europe, aims to directly compete with U.S. mega-constellations.

However, Chinese satellite ambitions, while formidable, are likely to remain regionally focused and face challenges in capturing global markets. Chinese satellite systems, such as the BeiDou navigation network, are historically designed for domestic use and strategic regional influence through initiatives like the Digital Silk Road.

These systems are often bundled into infrastructure packages offered to friendly nations in Africa, Latin America, and Southeast Asia, where China seeks to expand its geopolitical and economic influence.[24]

Unlike U.S. operators, Chinese satellite providers face hurdles in global adoption due to less

[20] Santiago Rementeria, Power Dynamics in the Age of Space Commercialisation, Space Policy, Volume 60, 2022, 101472, ISSN 0265-9646, https://doi.org/10.1016/j.spacepol.2021.101472.

[21] Abels, J. (2024). Private infrastructure in geopolitical conflicts: the case of Starlink and the war in Ukraine. *European Journal of International Relations*, *30*(4), 842-866. https://doi.org/10.1177/13540661241260653 (Original work published 2024)

[22] https://www.newspace.im/constellations/amazon

[23]https://www.iiss.org/online-analysis/six-analytic-blog/2025/05/orbital-ambitions-leo-satellite-constellations-and-strategic-competition/

[24] https://jamestown.org/the-beidou-satellite-network-and-the-space-silk-road-in-eurasia/

competitive pricing, limited interoperability with global standards, and concerns over data security and state control, which deter widespread B2B and B2C uptake in competitive markets.

Finally, both the U.S. and Chinese solutions are increasingly vertically integrated, controlling the entire value chain from satellite manufacturing to insurance, launch and operations.

However, the U.S. have an advantage over China: SpaceX’s reusable Falcon and Starship systems and Blue Origin’s New Glenn. The global market penetration and commercial flexibility of these systems, which dominate launch services with cost-effective, reusable rockets, drive down costs and enable rapid deployment.

China’s launch ecosystem, while robust and supported by a domestic launcher ecosystem that already fields more than 20 consolidated companies, is less cost-competitive and primarily serves state-driven objectives.[25]

As a result, while China’s satellite networks may achieve regional dominance and support strategic goals in allied nations, the U.S. is likely to maintain its global lead in satellite communications through superior scale, market-driven innovation, and broader commercial appeal.

3.3 What about Europe? IRIS² and OneWeb: opportunities and challenges

Europe’s commercial presence in LEO today rests mainly on OneWeb: originally financed by European and Japanese investors and now controlled by the French Eutelsat, it operates a 648-satellite first-generation constellation, with a second generation under development.

However, OneWeb is neither able to compete technologically with U.S. and Chinese operators nor does it enjoy a strong financial position: in June 2025, South Korea’s Hanwha Systems sold its 5.4% Eutelsat stake at a significant discount.

The French government, despite the financial turmoil it is currently facing, responded with a €1.35 billion capital injection, becoming the company’s largest shareholder with nearly 30% of the capital, aiming to stabilise the group after the costly OneWeb acquisition.[26]

The EU’s main structural response to this lag in satellite communications is IRIS², launched in 2022 and conceived as the Union’s third space flagship project after Galileo and Copernicus. IRIS² is designed as a multi-orbit architecture with 274 satellites in LEO and an additional 18 in MEO, with also several GEO satellites to reinforce the infrastructure, all capable of interconnecting to provide redundancy and flexibility.[27]

The programme is run by the SpaceRISE consortium) – SES, Eutelsat, Hispasat, Airbus, Thales Alenia Space, OHB, Orange, Deutsche Telekom – as a public-private partnership (PPP) with the European Commission (DG DEFIS). The initial budget was €6 billion, but it has jumped to more than

[25] https://www.iiss.org/online-analysis/charting-china/2025/08/chinas-commercial-space-sector

[26] https://www.defensenews.com/global/europe/2025/06/20/eying-a-starlink-alternative-france-to-boost-eutelsat-stake/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru ; https://spacenews.com/eutelsat-orders-100-leo-satellites-to-replenish-oneweb-constellation ; https://www.defensenews.com/global/europe/2025/06/20/eying-a-starlink-alternative-france-to-boost-eutelsat-stake/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru

[27] https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2

€10 billion, half of which is public funding, due to increasing costs. Moreover, initial services, announced for 2026-2027 are expected realistically after 2030-2032.

Besides rural broadband and maritime links, IRIS^2 aims to support secure communications for crisis response, border surveillance, diplomatic networks, and - marginally - military functions.

A defining feature of IRIS^2 is its integration with EuroQCI, launched in 2019 to deploy a dual fiber and space quantum network. Through Quantum Key Distribution (QKD), IRIS^2 aims to provide ultra-secure communications and full interoperability with 5G and future 6G networks.

Yet its capacity remains extremely limited: the system aims for 3.3 Tbps by 2032, which is too small compared with American and Chinese mega-constellations.[26] By 2035, several new LEO networks will intensify global competition and reduce prices: Europe will not be competitive enough in the commercial landscape.

The recent trend towards dual-use applications, and the recent NATO agreement on 5% defense spending on GDP, has prompted new national initiatives across Europe.

Italy announced a LEO satellite military constellation of more than 100 satellites by 2031[28] with an initial budget of €765 million,[29] reflecting both ambition and also budget constraint and efficiency challenges in defence spending.

Germany, with a plan to spend over €40 billion on space in the next years,[30] proposed a national LEO constellation of hundreds of satellites for military and governmental use by 2030. With the largest fiscal capacity in the EU and the biggest absolute increase in defense spending, Germany has the widest potential to invest in such projects.[31]

These systems can reinforce Europe's satellite infrastructure – especially where IRIS^2 offers limited military capabilities – if effectively integrated. They may also support regional resilience: Italy's constellation could strengthen Mediterranean and Africa-bound connectivity; Germany's programme could reinforce the Baltic and Northern Europe, regions exposed to hybrid threats; and France's role in OneWeb, combined with participation in IRIS^2, ensures substantial commercial and government capacity across the continent.

Together, they can provide redundancy for critical data now concentrated in vulnerable SCCs. However, the lack of coordination and the fragmentation of projects make impossible to exploit economies of scale.

Furthermore, the focus on national projects risk jeopardising European efforts, contributing to the increasing uncertainty on projects like IRIS^2, with several delays and costs increases[32].

Industrial policy adds another piece to the puzzle. The EU has launched Project BROMO to consolidate satellite manufacturing capabilities, reduce fixed costs, and exploit economies of scale and scope across telecommunications, EO, navigation, IoT, and scientific missions.

[28] https://www.reuters.com/business/media-telecom/italy-moves-phase-2-satellite-constellation-plan-2025-03-31/

[29] https://spacenews.com/italys-crossroads-build-its-own-satellites-or-lean-on-starlink-while-waiting-for-iris%C2%B2/

[30] https://spacenews.com/what-germanys-41b-investment-in-space-could-mean-for-europe/

[31] https://www.space.com/space-exploration/satellites/germanys-military-wants-its-own-starlink-like-satellite-constellation

[32]https://www.kratosspace.com/constellations/articles/at-esa-ministerial-conference-a-possible-german-competitor-to-europes-iris2-with-germanys-investment

Its approach follows the Draghi Report (2024), which calls for joint procurement and co-production instead of fragmented national projects. This strategy supports technological interoperability, cross-border industrial synergies, and strategic autonomy.

Still, Europe will not match the scale of US or Chinese constellations without more satellites, deeper vertical integration and especially a stronger launch sector.

Currently, Europe lacks a reusable launcher, and it is continuing to invest in non-reusable launchers such as Ariane and Vega, which rely on solid propellants used by French ballistic missiles.

This choice ensures synergies with the defense industry, especially in France, at national level, but has so far left Europe technologically behind in the global shift toward reusable, liquid-fuelled rockets.

The French launcher Ariane 6, which had a successful first commercial flight in March 2025, can deploy only a fraction of what Falcon 9 or Starship will lift annually.[33] More ambition and cooperation from EU are required on this side.

However, at the same time, resilient connectivity does not necessarily require tens of thousands of LEO satellites. If national programmes move quickly and IRIS² comes online with advanced technology from 2030 onward, the combination of new military constellations, OneWeb's reinforcement, and IRIS²'s secure services could provide the level of redundancy and autonomy required for a resilient European satellite communications architecture.

3.4 Strategic implications for Europe

Russia's full-scale invasion of Ukraine in February 2022 showed how exposed Europe is in satellite communications. The cyberattack on KA-SAT, Viasat's network used across Ukraine and parts of Europe, disabled thousands of modems and pushed Ukraine to rely on Starlink, which SpaceX activated within days.[34]

But dependence on a private U.S. system carries political and operational risks: a 2025 Reuters investigation reports that Elon Musk ordered Starlink to deactivate coverage during the 2022 counteroffensive, shutting down at least 100 terminals and disrupting Ukrainian drone and artillery coordination.[35]

OneWeb offers some diversification, yet its smaller constellation and ground network cannot match Starlink's responsiveness. These vulnerabilities are compounded by environmental risks.

The rapid expansion of large constellations increases the probability of Kessler-style[36] debris cascades.

[33] Di Pippo, S. (2025) Space Economy – L'arena competitiva del futuro. 2nd edn. Milan: Egea Spa – Bocconi University Press

[34] https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

[35]https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/

[36] More formally known as the Kessler Syndrome, is a theoretical cascade in space where the density of orbital debris becomes so high that collisions generate even more debris, creating a runaway chain reaction that could render Low Earth Orbit unusable for satellites and space missions for generations (Kessler, 1978).

.

The EU has begun addressing this through the 2021 EU Space Programme with Space Situational Awareness (SSA) project and through forthcoming rules in the EU Space Act, which will tighten debris mitigation, collision avoidance, and cybersecurity requirements.

ESA’s debris-removal missions and the future EU Space Traffic Management framework reinforce this effort.

A third risk comes from anti-satellite (ASAT) weapons. India, Russia, China, and the United States have all demonstrated kinetic or electronic ASAT capabilities, from jamming and spoofing to GPS interference and direct-ascent missile tests, which increase the debris in space.

LEO constellations are harder to disable completely but easier to target individually, while GEO systems face persistent electronic warfare. For Europe, which relies heavily on commercial and foreign-owned platforms, ASAT threats make resilience, redundancy, and multi-orbit architectures essential.

These challenges raise a strategic question: in a market soon dominated by U.S. and Chinese mega-constellations offering vast capacity at low prices, what future awaits European systems like IRIS^2 and OneWeb if demand does not expand accordingly?

The EU is investing billions in SATCOM programmes while global attention shifts toward defence constellations. Yet governance remains fragmented between the Commission, EUSPA, ESA, EDA, national space agencies and governments, complicating Europe’s ability to coordinate investments and secure genuine strategic autonomy.

4. How do satellites complement cables? Use cases, policies and recommendations for a stronger EU telecommunication infrastructure

Cables and satellites can work together for a more resilient and efficient telecommunication infrastructure. In this final chapter we will analyse some use cases, where satellites demonstrated to be complementary to cables after disruptions.

We will analyse more in detail the NATO’s HEIST project, which aims to create a hybrid architecture combining cable and satellite capabilities. We conclude with some recommendations for European policymakers.

4.1 How satellites and cables work together

Satellites have demonstrated on several occasions to be an indispensable complement to submarine cables.

When SCCs fail, entire countries and regions can be pushed into digital isolation unless a resilient backup is in place, and in this paragraph, we will see some examples.

Firstly, when the only undersea cable of the Pacific Island state of Tonga was damaged in 2019 and

again destroyed by the volcanic eruption in 2022, the country was effectively cut off from the world.[37]

In 2019, only the rapid activation of satellite connectivity, particularly with the satellite broadband provider Kacific, allowed Tonga to restore basic communication services until repairs were completed weeks later.

In 2022, shortly after the second eruption, SpaceX donated 50 Starlink terminals to reestablish the island's internet connectivity while the complete repair of the SCC took more than a month.[38]

In 2024, SCC cuts in the Red Sea and major outages in West and Central Africa forced operators such as CMC Networks to fall back on multi-orbit constellations, drawing on satellites to keep data flowing.[39]

Finally, in 2025, Taiwan faced repeated undersea cable disruptions, such as the Keelung and Penghu incidents in January and February, with increasing threat from China. With only 14 SCCs connecting the island to the rest of the network, these disruptions exposed its digital vulnerabilities.[40]

So far, traffic was rerouted through alternative SCCs, but these events accelerated plans to integrate satellites as a "Plan B" for secure redundancy.[41]

With respect to Europe, the High North offers another example of this interdependence. Svalbard's satellite ground station relies entirely on two long fibre links to mainland Norway.

When one of these cables was damaged in 2022, the island's capacity dropped immediately. Studies on Svalbard system show that neither satellites nor cables can function in isolation there: satellites cannot replace the fibre backbone, but they provide the only temporary lifeline when a fault occurs, while the cables carry the heavy traffic that satellites cannot handle.[42]

These episodes underscore that, even with a limited bandwidth, satellites provide flexibility, rapid deployment, and coverage in areas where SCCs are absent or too fragile, making them a crucial pillar of redundancy in telecommunications.

Taiwan or Tonga show just how exposed territories like islands can be when their SCCs are disrupted. Their responses matter for our analysis, since Europe, from High North to the Mediterranean and in the Atlantic is dotted with islands and archipelagos that carry strategic military, economic, and scientific value.

Moreover, other fragile areas like the Baltic States can themselves be seen as a peninsula-like region from a cable's point of view: connected to continental Europe only through a narrow land corridor with Poland, they face vulnerabilities to cable disruptions that resemble those of an island.

[37] https://csps.aerospace.org/sites/default/files/2022-02/Gordon-Jones_UnderseaCables_20220201.pdf

[38] https://www.theguardian.com/world/2022/jan/21/elon-musk-starlink-internet-tonga-volcano

[39] https://www.capacitymedia.com/article/2cxwfv3edqrmwybmbrtaa/news/red-sea-cable-cuts-sees-organisations-turn-to-satellite-connectivity

[40] https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities/

[41] https://globaltaiwan.org/2025/07/a-plan-b-for-prc-cable-cutting

[42] Boschetti, Nicolò & Falco, Gregory. (2025). Underwater Cyber Warfare: Submarine Communications Cables Architecture and Cybersecurity Analysis. 10.24251/HICSS.2025.233

4.2 Cables and Satellites, toward a Hybrid Architecture: NATO project HEIST

NATO's Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunications (HEIST) is the clearest example of how satellites and cables can be integrated into a single resilient architecture.

In the HEIST model, submarine cables are equipped with fiber-based monitoring tools – such as the above-mentioned DAS, maritime surveillance assets, and digital intrusion-detection systems – that can detect faults or sabotage within meters.

When an incident occurs, HEIST triggers an immediate, automated response: high-priority traffic is rerouted through satellite networks until the cable is repaired. The innovation lies in the introduction of the following governance architecture for transatlantic SCCs, not just a technical function:

- Situational awareness hubs gather real-time information from subsea sensors;
- Smart contracting layers automatically activate emergency service level agreements with satellite providers through secure, automated blockchain-based contracts;
- A satellite ecosystem of multiple operators – Starlink, OneWeb, SES O3b, Amazon Leo – provides temporary high-priority capacity even if providers have no pre-existing agreements.

Simulation results from the HEIST study show that this architecture can successfully reroute high-priority traffic during cable failures, dynamically redistributing loads across multi-orbit, multi-operator constellations. For Europe, this hybrid logic matters for three reasons.

- Europe cannot rely solely on SCC redundancy, especially in chokepoints or between islands and mainland. The HEIST approach offers a realistic insurance layer that buys time until cable repairs are completed.
- Satellites are entering a phase of exponential growth, but their capabilities vary across orbits. LEO constellations offer low latency; MEO systems like O3b mPOWER deliver enterprise-grade capacity; GEO provides persistence. A hybrid cable–satellite architecture deliberately combines these strengths, offering continuity of service even in geographically isolated regions. This is particularly relevant for EU islands, peripheral Member States, and overseas territories, where single-cable dependencies persist.
- HEIST provides a governance framework Europe currently lacks. By using smart contracts, pre-negotiated priorities, and automatic activation triggers, it avoids bureaucratic delays in the middle of a crisis. This is critical for transatlantic security: a disruption to major EU–US cables could instantly degrade financial transactions, cloud services or cross-border data flows. A HEIST-style architecture for Europe, and not only for Transatlantic SCCs, ensures that at least critical data continues to flow, even under coordinated attacks.

The strategic takeaway is clear: cables for now remain irreplaceable, satellites make them resilient, and Europe with the announced national military constellations, IRIS^2 and OneWeb could aim to have its own HEIST system.

4.3 Recommendations and policies for EU

In this section, we advance a set of recommendations aimed at better strengthening Europe's connectivity and, in particular at addressing the vulnerabilities of its undersea cables and its satellite communications

- *Cable-satellites integration*. Following the experience of NATO Project HEIST, European countries should define traffic prioritisation protocols for European critical cables – using the very Project HEIST as a framework and expand it to European cable and satellite systems.

These protocols should be nationally implemented but coordinated at the EU level and tested in joint drills also with NATO and other non-EU private and public actors. This will facilitate redundancy and resilience through cooperation and investments in satellite-cables complementarity with significant implications also for innovation.

- *IRIS^2 or quality over quantity*. IRIS^2 will not be able to compete commercially with U.S. entities. However, it could play a vital role for government, diplomatic and military applications.

For this reason, European countries should consolidate satellite data capacity for strategic, military, and emergency use, to complement cables and support in the event of disruption.

In this respect, many European countries are launching national (military) constellations. On the one hand, they will add redundancy. On the other, they are unlikely to be substitutes and rather they will serve as complements of IRIS^2.

Given that the government, diplomatic and military traffic on LEO constellations is limited, there is potential scope for intra-European cooperation, from the very constellations, the production of satellites and software applications for integration and cooperation.

Arguably, a single European constellation can be larger, cheaper and more secure than individual national constellations. In short, a possible solution could be switching from a PPP model for IRIS^2, to a fully public model, with a focus on government and military services.

- *Private actors*. The new space age is characterized by the growing role of private actors. For this reason, European countries should facilitate procurement and co-production for private space operators within the EU, following the example of project BROMO, creating real European champions and boosting productivity and competitiveness.
- *The effectiveness of inefficiency in defense*. The protection of undersea cables is expensive and subject to diminishing marginal returns. However, European countries should launch other Baltic Sentry-like missions with the twin goal of funding innovative technological solutions as well as complicating its adversaries' calculus and operations.

In particular, by adopting flexible, randomized patrolling operations, varying intensity, methods and critical areas, European countries can make adversarial attacks significantly more difficult.

- *The deterrence of resilience*. Repairing undersea cable is complex and expensive. This, potentially, raises an adversary's payoff to attack them. European countries should then establish fast-track repair corridors with pre-cleared maritime routes and standardized legal templates for emergency authorisations for repairing vessels. This prevents delays linked to national permitting procedures in the event of cable disruption.

Bibliography

- Di Pippo, S. (2025) *Space Economy – L'arena competitiva del futuro.* 2nd edn. Milan: Egea Spa – Bocconi University Press
- Boschetti, Nicolò & Falco, Gregory. (2025). Underwater Cyber Warfare: Submarine Communications Cables Architecture and Cybersecurity Analysis. 10.24251/HICSS.2025.233
- Boschetti et al. (2025). Hybrid Space and Submarine Architecture to Ensure Information Security of Telecommunications (HEIST). IEEE Access. PP. 1-1. 10.1109/ACCESS.2025.3631359.
- Romano, Fabio, FROM SEA TO SPACE Satellites as a Backup for Undersea Cables https://www.enisa.europa.eu/sites/default/files/2025-03/9%20-%20ENISA%20-%20Fabio%20ROMANO%20SES%20-%20Amsterdam%2020%20March%202025.pdf
- https://bisi.org.uk/reports/strategic-alliance-of-sea-and-space-synergies-between-subsea-cables-and-leo-satellites
- Marcus Solarz Hendriks and Harry Halem. From space to seabed Protecting the UK's undersea cables from hostile actors. Policy Exchange (2023) https://policyexchange.org.uk/wp-content/uploads/From-space-to-seabed.pdf
- Lori W. Gordon & Karen L. Jones, Global Communications Infrastructure: Undersea and Beyond. The Aerospace Corporation, Center for Space Policy and Strategy (2022).
- https://elliott.gwu.edu/undersea-cables-and-vulnerability-american-power
- Niels Nagelhus Schia, Lars Gjesvik and Ida Rødningen. Loss of Tonga's telecommunication: What happened, what were the consequences and how were they managed? Norwegian Institute of International Affairs (2022).
- A. Blechová, "The Next Step in Global Connectivity: Legal Challenges in the Shift from Subsea Cables to Satellites," 2025 17th International Conference on Cyber Conflict: The Next Step (CyCon), Tallinn, Estonia, 2025, pp. 39-55, doi: 10.23919/CyCon65856.2025.11103582
- J. Michael Dahm (2020). South China Sea Military Capability Series A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea, UNDERSEA FIBER-OPTIC CABLE AND SATELLITE COMMUNICATIONS, John Hopkins University https://www.jhuapl.edu/sites/default/files/2022-12/UnderseaFiber-OpticCableandSATCOM.pdf
- Frank Rayal, Xona Partners Dr. Riad Hartani, Xona Partners Artur Mendes, Angola Cables. Defining the Synergies between LEO Satellite Constellations and Submarine Cables (2020) https://xonapartners.com/wp-content/uploads/2020/12/Defining-the-Synergies-between-LEO-Satellite-Constellations-and-Submarine-Cables.pdf
- https://www.subseacables.net/reports-and-coverage/satellites-vs-subsea-navigating-asias-future-of-connectivity/
- https://repository.globethics.net/server/api/core/bitstreams/72b033d1-2f57-4e13-9f98-0658d8876bd8/content
- https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables
- https://www.colt.net/resources/the-future-of-global-connectivity-through-the-hybrid-power-of-leo-satellites-and-submarine-cables/

APPENDIX

A. Non exhaustive list of the main disruptions affecting SCCs in Northern Europe in chronological order.

Date	Cable (location)	Nature	Description
3 Apr 2021	**Svalbard Undersea Cable System (Nigh North and Arctic)**	Unknown vessel type. Causes: unknown; suspected sabotage	The LoVe Ocean Observatory in northern Norway abruptly lost connection when several kilometers of its SCCs were mysteriously severed and removed, leaving critical monitoring platforms inoperative. Investigations confirmed the cables had been dragged far from their original route, suggesting deliberate human interference. The case remains under police and security service investigation.
20 Oct 2022	**SHEFA-2** (North Sea)	Fishing vessel involved. Causes unknown; accident	Connectivity was rerouted via older links (like FARICE-1) and restored within a few days.
7 Jan 2022	**Svalbard Undersea Cable System (Nigh North and Arctic)**	Fishing vessel involved. Causes: unknown; suspected sabotage	Police located seabed marks via remote vehicle; no sabotage charges were filed, and no deliberate intent was established. Repairs were completed later in 2022 with the help of a cable-laying vessel.
7-8 Oct 2023	**Sweden-Estonia EE-S1 (Baltic Sea)**	Unknown vessel type involved. Causes: anchor drag; suspected sabotage	Investigations revealed anchor drag marks and an embedded anchor consistent with the movements of a nearby vessel, the Hong-Kong-flagged Newnew Polar Bear. Authorities suspect the damage was intentional or, at the very least, highly negligent.
18 Nov 2024	**BCS East-West Interlink (Baltic Sea)**	Merchant vessel involved. Causes: anchor drag; suspected sabotage	The Chinese bulk carrier Yi Peng 3, which left the Russian port of Ust-Luga three days prior, was quickly identified as the culprit and stopped by Danish authorities on the Kattegat sea. After China initially refused investigators permission to board the vessel, it was allowed to continue its journey on December 21st. The investigation is still ongoing.
18 Nov 2024	**C-Lion1 (Baltic Sea)**	Merchant vessel involved. Causes: anchor drag; suspected sabotage	Just a few hours after the BCS East-West Interlink between Sweden and Lithuania is severed, the C-Lion1 Data cable between Finland and Germany suffers the same fate. The break is quickly linked to the same vessel, Yi Peng 3.
25 Dec 2024	FEC-1, FEC-2, Baltic Sea Submarine Cable, C-Lion1 **(Baltic Sea)**	Merchant vessel involved. Causes: anchor drag; suspected sabotage	Tanker Eagle S, a Cook Islands–registered vessel, is responsible. Authorities allege this incident involved sabotage or at least highly negligent behavior, as the vessel continued in the area after the cables and nearby Estlink 2 power cable were severed (probably the real objective of the suspected sabotage). Repairs to the cable were complete by January 6, 2025, with full restoration by mid-2025.

26 Jan 2025	Sweden-Latvia **(Baltic Sea)**	Merchant vessel involved. Causes: anchor drag and adverse weather conditions; accident	The Malta-flagged carrier Vezhen and Norwegian-flagged but Russian-operated Silver Dania are initially suspected and apprehended by Swedish and Norwegian authorities, but all suspicions of deliberate sabotage are later dropped. There were no reported interruptions to communications.
26 Jan 2025	C-Lion1 **(Baltic Sea)**	Unknown vessel type. Causes: failure; unknown intentions	In February 2025, the cable operator Cinia detected a disturbance on the C-Lion1. The disturbance did not affect the functionality of telecommunications connections within the cable. The damage likely occurred on 26/01 during the cable damage involving the Sweden–Latvia cable but was only detected in late February. The investigation remains ongoing, though the cable has already been repaired.
27 Jul 2025	**SHEFA-2** (**North Sea**)	Fishin vessel involved. Causes: anchor drag; unknown intentions	The SHEFA-2 subsea fibre cable, which connects Orkney and Shetland with mainland Scotland and onward to the Faroe Islands, suffered a major break, leaving hundreds of homes and businesses in Shetland and Orkney without broadband, although landline telephones continued to function. The disruption lasted several days, as repair ships were mobilised to locate and retrieve the damaged section of cable before installing replacements. Local operators described the fault as “serious but not unprecedented”.

Sources:https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/; https://gbv.wilsoncenter.org/article/mapping-undersea-infrastructure-attacks-baltic-sea; https://go.recordedfuture.com/hubfs/reports/ta-2025-0717.pdf.

B. Non-exhaustive list of the main LEO, MEO, and Multi-Orbit constellations operative and under development, study or announced, as of September 2025

Constellation	Company/Provider	Country	First Launch	Planned Size	Level of Security	Orbit
Starlink	SpaceX	US	2018	25,000-42,000	COM	LEO
Qianfan	Shanghai Spacecom Satellite Technology	China	2024	15,000	COM	LEO
Guowang	China Satellite Network Group (SOE)	China	2023	13,000	GOV + MIL	LEO
Honghu - 3	Hongqing Technology	China	n.d.	10,000	MIL	LEO
Amazon Leo (former project Kuiper)	Amazon	US	2023	3,236	COM	LEO
Meridian	Spinlaunch	US	n.d.	1,200	COM	LEO
OneWeb	OneWeb (Eutelsat)	France	2026*	748**	COM + GOV + MIL	LEO
SDA's Transport Layer	Space Development Agency (SDA)	US	2022	500	MIL	LEO
Starshield	SpaceX	US	2020	400	MIL	LEO
IRIS^2	SpaceRISE Consortium	EU Member States	2027	292	COM + GOV + MIL	LEO + MEO + GEO
AST Spacemobile	AST SpaceMobile, Inc.	US	2019	243	COM	LEO
Lightspeed	Telesat + Space Norway	Canada	2026	198	COM	LEO
Iridium NEXT	Iridium Communications Inc.	US	2019	75	COM	LEO
O3b mPOWER	O3b Networks (SES)	Luxembourg + UK	2022	13	COM	MEO

*Second generation. **First generation (648 satellites) + second generation (at least 100 satellites)

Source: EUSPA Secure Satcom Market Report, 2023; EUSPA GNSS and Satcom User Technology Report, 2025; additional sources from single operators' websites and articles.

.