Strengthening the Resilience of Submarine Cables in the Atlantic: A Capability-Driven Approach

1. Introduction

Abraham Maslow's well-known hierarchy of needs teaches us that at the base of human priorities lie physiological necessities such as food, water, and shelter. Yet immediately above them, forming the second most fundamental layer, stands something societies often underestimate and too frequently take for granted: **security**. Physical security. Stability. Protection. Predictability. These precede recognition, self-actualisation, economic growth, and even innovation. Their primacy should prompt us to pause and reflect on their true significance. If Maslow were alive today, he would likely adjust his pyramid to include **connectivity** among the essential early layers, acknowledging that modern societies have come to depend on uninterrupted digital access as a basic condition for functioning.

This reflection is not merely philosophical. It is profoundly material. The modern world's connectivity flows through a largely invisible infrastructure: **submarine cables**, the physical backbone of the global digital ecosystem. These systems carry more than 95% of intercontinental data traffic, enabling financial markets, cloud services, defence communications, scientific cooperation, and the daily functioning of contemporary societies. Nowhere is this more strategically relevant than in the Atlantic basin, where Europe, Africa, and the Americas are bound together by a dense yet vulnerable network of fibre-optic systems.

Despite their centrality to modern life, submarine cables have long been treated as technical assets rather than strategic components of national and collective security. This assumption no longer holds. Recent geopolitical tensions, hybrid threats, and the increasing militarisation of the seabed have exposed the fragility of the Atlantic's digital arteries. What was once perceived as a stable and secure environment is now a theatre of state-sponsored interference, covert seabed operations, and accidental or deliberate disruptions.

Against this backdrop, the resilience of submarine cables must be understood not only as a technical challenge but as a **strategic imperative**. This paper frames cable resilience through the lens of **Information Security**, **Resilience**, and the EU's evolving regulatory framework, particularly the NIS2 Directive[1] (EU 2022/2555) and the CER Directive[2] (EU 2022/2557). It then connects these foundations to

[1] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1767864030175

recent strategic documents, including the EU Recommendation 2024/779[3], the 2025 Joint Communication to strengthen the security and resilience of submarine cables[4], the EU Report on Submarine Cable Security and Resilience (2025)[5], the 2026 Porto Declaration[6], and EuroStack 2025[7], before concluding with a capability-driven set of recommendations structured according to the DOTMLPFI[8] model.

Submarine cables are inherently **cyber-physical systems**, and their protection requires an integrated approach that spans cybersecurity, maritime and energy security, regulatory governance, and international cooperation. As this paper argues, infrastructure, technology, and regulation are necessary but insufficient. The decisive factor is **governance**, i.e., the integrating capability that aligns actors, its mandates, and operational responsibilities across the Atlantic basin.

2. Information Security as a Foundation for Cable Resilience

Information Security is traditionally defined as the ensemble of **processes, people, and technologies** that ensure the **Confidentiality, Integrity, and Availability (CIA)** of information. When applied to submarine cables, this framework reveals a multidimensional challenge:

- **Confidentiality**: Submarine cables can be tapped using repeaters or seabed interception devices, enabling espionage or data exfiltration.
- **Integrity**: Physical tampering, signal manipulation, or cyber interference with landing stations can compromise data integrity.
- **Availability**: Cable cuts, whether accidental, natural, or intentional, can disrupt connectivity, with cascading effects on critical services. The same effect may be produced by a power outage, regardless of its origin.

The **NIS2 Directive (EU 2022/2555)** significantly expands this perspective by classifying **electronic communications networks and services**, including

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400779

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

[5] https://digital-strategy.ec.europa.eu/en/library/report-security-and-resilience-eu-submarine-cable-infrastructures

[6] https://www.itu.int/digital-resilience/submarine-cables/wp-content/uploads/sites/2/2026/02/Porto-Summit-Declaration.pdf

[7] https://www.euro-stack.info/docs/EuroStack_2025.pdf

[8] *Capability is a concept that defines the ability to create a desired effect, integrating Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI) into a cohesive system, moving beyond mere equipment to encompass the entire lifecycle, from policy (driven by threats) to development, deployment, and adaptation, focusing on future potential rather than specific adversaries.*
(https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3800/RRA3831-2/RAND_RRA3831-2.pdf)

submarine cable operators and landing stations, as **essential or important entities**. This imposes obligations for:

- **risk management**,
- **incident reporting**,
- **supply-chain security**,
- **business continuity**,
- **cyber-physical integration**.

In parallel, the **CER Directive (EU 2022/2557)** introduces a broader concept of **resilience of critical entities**, requiring Member States to identify and protect operators whose disruption would have significant societal impact. Submarine cable landing stations, network operation centres, and repair facilities fall squarely within this logic.

Together, NIS2 and CER create a **dual regulatory foundation**:

- **NIS2** → cyber and operational security of digital infrastructure
- **CER** → physical resilience and continuity of critical entities

This duality is essential for submarine cable systems, which are inherently **cyber-physical**.

3. Energy Dependencies of Digital Infrastructure

Submarine cables and the wider digital ecosystem depend on a stable and resilient energy system. Landing stations, optical amplifiers, data centres, and network operation facilities require continuous, high-quality electricity. As the document notes, submarine cables are "inherently cyber physical systems" and their protection "requires an integrated approach" across domains, energy included.

The digital transition is increasing electricity demand, particularly through AI workloads and hyperscale cloud interconnection. At the same time, the energy transition introduces new vulnerabilities. Renewable energy variability, grid instability, and climate driven extreme weather can all disrupt power supply to critical digital nodes. A loss of power at a landing station can have the same effect as a physical cable cut, hence hampering cable availability, which yields an information security incident.

Conversely, the energy system itself is becoming more digitalised, creating a mutual dependency. A cyber incident affecting energy systems can cascade into digital infrastructure, while a disruption of submarine cables can impair the digital services that manage energy balancing.

Energy resilience therefore becomes a foundational layer of cable resilience. It ensures continuity of power, enables redundancy through storage and microgrids, and supports rapid recovery during crises. Without energy resilience, digital resilience cannot be achieved. The 2025 Iberian Peninsula power outage is a obvious example of this interdependencie.

4. From Security to Resilience

Resilience extends beyond protection. It encompasses the **capacity to anticipate, withstand, recover from, and adapt to disruptions**. For submarine cables, resilience includes:

- **Redundancy** (multiple routes, diverse landing points and energy sources)
- **Robustness** (physical protection, secure landing stations)
- **Rapidity** (fast repair cycles, simplified authorisations)
- **Adaptability** (dynamic routing, situational awareness, cross-domain coordination)

The **CER Directive** reinforces this by requiring Member States to:

- conduct **national risk assessments**,
- identify **critical entities**,
- ensure **resilience measures**,
- support **cross-border cooperation**.

Meanwhile, **NIS2** mandates that operators adopt **state-of-the-art cybersecurity and incident-response capabilities**, which are indispensable for cable landing stations and network management systems.

Thus, the transition from security to resilience is not conceptual alone—it is **legally mandated**.

5. Policy and Strategic Context

Recent years have seen a surge of strategic attention to submarine cable resilience. Several documents provide a coherent framework that directly informs Atlantic security.

5.1. EU Recommendation 2024/779 on Secure and Resilient Submarine Cable Infrastructures

This is the first EU-level instrument dedicated exclusively to submarine cables. It:

- Recognises cables as **critical infrastructure essential to EU sovereignty**.
- Identifies threats from **state actors**, **hybrid operations**, and **physical sabotage**.
- Calls for **risk assessments**, **redundancy**, and **cross-border coordination**.
- Encourages Member States to streamline **repair authorisations** and **maritime procedures**.

It explicitly builds on **NIS2** and **CER**, positioning submarine cable resilience within the EU's broader critical-infrastructure architecture.

5.2. Joint EU Communication on Strengthening Submarine Cable Security (2025)

This document operationalises the 2024 Recommendation by proposing:

- A **basin-based monitoring model** (Baltic, Mediterranean, Atlantic).
- Enhanced **maritime domain awareness** for seabed infrastructure.
- A European mechanism for **rapid repair and crisis coordination**.
- Integration with NATO and like-minded partners.

It also reinforces the **NIS2/CER duality**, emphasising cyber-physical integration.

5.3. EU Report on Submarine Cable Security and Resilience (2025)

This technical report provides:

- A **complete mapping** of EU cable infrastructure.
- A **stress-test methodology** for physical and cyber risks.
- Recommendations for **redundancy**, **landing station security**, and **supply-chain integrity**.

It explicitly references **NIS2 risk-management obligations** and **CER resilience requirements**.

5.4. Porto Submarine Cable Resilience Summit Declaration (2026)

Adopted at the 2026 Summit hosted by ANACOM, ITU, and ICPC, the declaration emphasises:

- **International cooperation** and **shared situational awareness**.
- Reduction of **bureaucratic barriers** to cable repair.
- Creation of **national Single Points of Contact**.
- Promotion of **geographical diversity** in landing points.

5.5. EuroStack 2025

Although not focused solely on cables, EuroStack recognises **undersea cables** as part of Europe's **sovereign digital infrastructure layer**. It highlights:

- The need for **European jurisdiction** over critical digital assets.
- The role of **Alcatel Submarine Networks** and other European actors.
- The importance of **secure connectivity** (EuroConnect MVP).
- The link between cable resilience and **digital autonomy**.

EuroStack aligns naturally with **NIS2's cybersecurity obligations** and **CER's resilience requirements**, reinforcing the need for a **sovereign, secure, and resilient Atlantic digital backbone**.

6. The Atlantic as a Strategic Environment

The Atlantic basin presents unique challenges and opportunities:

- It hosts some of the **world's most important transoceanic cables**, linking Europe to North America, South America, and Africa.
- It is increasingly contested by **state actors** capable of seabed operations.
- It contains **deep-sea trenches** and complex topography that complicate surveillance.
- It is a region where **NATO, EU, and national authorities** overlap, creating both redundancy and fragmentation.

Portugal, the Azores, Madeira, the Canary Islands, Cape Verde, and the US East Coast form a **strategic triangle** for Atlantic cable resilience. The region is also a natural hub for **new-generation cables**, including those supporting cloud hyperscalers and scientific missions.

7. A Capability-Driven Approach to Submarine Cable Resilience (DOTMLPFI)

To move from policy to implementation, resilience must be framed as a **capability,** i.e., not merely as equipment or infrastructure, but as a **systemic ability to create a desired effect**.

Below is a structured set of recommendations aligned with the **DOTMLPFI** model, now explicitly linked to **NIS2** and **CER** obligations.

7.1. Doctrine (D)

- Establish a **European and Atlantic doctrine** for submarine cable protection and resilience.
- Integrate cable resilience into **national security strategies**, **maritime security doctrines**, and **cyber defence frameworks**.
- Align doctrine with **NIS2 risk-management principles** and **CER resilience requirements**.
- Adopt a **whole-of-society** and **whole-of-government** approach.

7.2. Organization (O)

- Create **national and regional coordination centres** for submarine cable security.
- Designate **Single Points of Contact** for repair authorisations, as encouraged by the Porto Declaration.
- Strengthen cooperation between **navies, coast guards, regulators, and operators**.
- Ensure organisational structures comply with **CER's critical-entity obligations**.

7.3. Training (T)

- Conduct **joint exercises** involving cyber, maritime, and telecom actors.
- Train operators and authorities in **incident response**, **seabed awareness**, and **hybrid threat detection**.

- Integrate cable scenarios into **NATO and EU exercises**, including NIS2-aligned cyber-incident drills.

7.4. Materiel (M)

- Invest in **redundant routes**, **diverse landing points and energy sources**, and **secure landing stations**.
- Deploy **seabed sensors**, **autonomous underwater vehicles (AUVs)**, and **AI-enabled monitoring**.
- Ensure **European supply-chain integrity**, consistent with NIS2's supply-chain security requirements.
- Pre-position repair vessels and spare parts in line with CER's continuity obligations.

7.5. Leadership (L)

- Promote political leadership that recognises cable resilience as a **strategic priority**.
- Encourage **Atlantic-wide partnerships**, including with the US, Canada, UK, and African coastal states.
- Foster leadership in **international standard-setting bodies** (ITU, ICPC, ENISA).
- Ensure leaders understand the **legal obligations** under NIS2 and CER.

7.6. Personnel (P)

- Develop specialised **subsea security teams** combining telecom, cyber, and maritime expertise.
- Strengthen the talent pipeline for **optical engineering**, **marine operations**, and **cyber-physical security**.
- Support retention through **career pathways** in critical infrastructure protection.

7.7. Facilities (F)

- Modernise **cable landing stations** with secure perimeters, redundancy, and physical hardening.
- Establish **Atlantic repair hubs** with pre-positioned vessels and spare parts.

- Ensure facilities meet **CER's physical-resilience requirements** and **NIS2's cybersecurity standards**.

7.8. Interoperability (I)

- Ensure interoperability across **EU, NATO, and private operators**.
- Harmonise **repair procedures**, **incident reporting**, and **security standards**.
- Promote **data-sharing frameworks** for maritime domain awareness.
- Align interoperability mechanisms with **NIS2's reporting obligations** and **CER's cross-border cooperation requirements**.

8. Conclusion

Submarine cables in the Atlantic are strategic assets whose disruption would have profound consequences for Europe's economy, security, and sovereignty. The emerging policy landscape (EU Recommendation 2024/779, the 2025 Joint Communication, the 2025 Technical Report, the 2026 Porto Declaration, EuroStack 2025, and the foundational NIS2 and CER directives) provides a strong foundation for action.

Yet **infrastructure, technology, and regulation alone are insufficient**.
The decisive factor for resilience is **governance**.

Governance is the **integrating capability** that binds together:

- the organisational structures needed for coordination,
- the leadership required for strategic direction,
- the legal mandates of NIS2 and CER,
- the operational responsibilities of public and private actors,
- and the cross-border cooperation essential in the Atlantic basin.

Without a **strong, coherent, and empowered governance structure**, the remaining DOTMLPFI components cannot achieve their intended effect.

A governance-centric approach ensures:

- **unity of effort** across cyber, maritime, diplomatic, and regulatory domains,
- **rapid decision-making** during crises,

- **alignment of incentives** between states and operators,
- **effective implementation** of EU directives,
- and **strategic coherence** across the Atlantic.

Only by embedding governance at the heart of the capability model can Europe and its Atlantic partners ensure that the digital arteries of the 21st century remain secure, resilient, and sovereign.

Looking ahead, these considerations must be understood in a pan Atlantic perspective. The European experience with NIS2, CER, and the emerging cable resilience architecture offers valuable lessons for other Atlantic partners, particularly in Africa and South America, where digital connectivity is expanding rapidly and where new subsea routes will shape the next decade of transoceanic infrastructure.

As Europe strengthens its governance, redundancy, and incident response mechanisms, similar approaches could support partner countries in developing their own resilience frameworks, ensuring that new investments in digital corridors are matched by robust security, energy stability, and operational continuity. At the same time, the expansion of South Atlantic and Africa Europe cable systems introduces additional challenges: longer repair times, limited regional repair capacity, greater exposure to extreme weather, and the need for interoperable governance across jurisdictions with different regulatory maturity. Existing North Atlantic routes also face increasing pressure from geopolitical competition, and the growing energy demands of digital infrastructure.

Therefore, a pan Atlantic approach that promotes shared situational awareness, coordinated crisis response, and harmonised resilience standards would undoubtedly strengthen not only Europe's security, but the stability and sovereignty of the entire Atlantic digital ecosystem.

Lisbon, the 1st of June 2026
António Gameiro Marques
Portuguese Navy RADM (Ret.)