OBSERVATÓRIO DOS ECOSSISTEMAS E INFRAESTRUTURAS DIGITAIS

2025

How to Increase the Resilience of Submarine Cables in Portuguese Waters?

CONTRIBUTIONS TO THE ELABORATION OF A NATIONAL STRATEGY

JOSÉ BARROS / LUÍS BERNARDINO

7 FEBRUARY 2025 - PORTUGAL

OBSERVATÓRIO DOS ECOSSISTEMAS E INFRAESTRUTURAS DIGITAIS

155 Years of Submarine Cables landing in Portugal, with Portuguese Waters being safe for Submarine Cables.

How to Increase the Resilience of Submarine Cables in Portuguese Waters?

Contributions to the elaboration of a National Strategy

José Sousa Barros

Chair of Advisory Board of Observatory of Ecosystems and Digital Infrastructures

Luís Manuel Brás Bernardino

President of Observatory of Ecosystems and Digital Infrastructures

Lisbon, February 7, 2025

INTRODUCTION

Submarine telecom cables (SCs) are the backbone of the modern global communication system. These fibre optic cables, which stretch for thousands of kilometres on the seabed, are responsible for transmitting about 98% of internet, voice, and video data between continents. SCs are vital, and therefore are a critical infrastructure.

Portugal, with its strategic geographical location in the interconnection between Europe, Africa, and the Americas, currently has about 10% of the total number of international SCs crossing its waters (this percentage is expected to grow significantly in the medium term). These cables are crucial for the resilience of the global telecommunications network.

The interruption of SCs can have significant economic impacts for Portugal and the world. Companies, financial institutions, and governments rely on secure and stable

connections for their daily financial operations. Any interruption can result in significant financial losses, in addition to affecting citizens' trust in a nation's or even the global telecommunications system.

The impact of SC interruption on society in general would also be devastating, with strong implications for the daily lives of every citizen, whether from a region or a country. It can jeopardize territorial and social cohesion and impact our safety.

Portugal's territorial cohesion also depends on the capacity for long-distance domestic interconnection, with SCs once again being fundamental for the CAM (Continent-Azores Is.-Madeira Is.) interconnection.

Portugal's sovereignty is conditioned by the control and diversification of international access. It is entirely convenient to have a wide variety of international access to the country so as not to be dependent on transits through a limited number of third countries to have access downstream from those countries. Once again, SCs are fundamental, and the more SCs that land in Portugal, the more diversity of international access we will have, the more options we will have, both in commercial terms and in terms of the quality of service to be contracted.

1. MAIN CAUSES FOR THE INTERRUPTION OF SUBMARINE CABLES

The main causes of interruptions on submarine cables are currently involuntary in (although there is evidence that this reality may be changing), and are due to causes that have been largely studied, namely:

(*) Natural Disasters (~14%) - SCs are vulnerable to several natural disasters such as landslides, earthquakes, tsunamis, storms, turbidity currents, abrasion, occasional cable suspension, etc. These events can damage or even disrupt CSs.

(*) Human Activities (~74%) - Fishing activities (trawling) and anchoring of vessels or floating platforms, and to a lesser extent dredging and the deposition of objects on the seabed, are responsible for damaging or interrupting SCs.

(*) Equipment Failures (~6%) - If the SCs have repeaters, it will require electrical and electronic equipment to be present on the seabed. Such equipment is designed and contracted to remain in operation for 25 years with a very low probability of failures occurring, however failures may occur. There is also electrical and electronic equipment in CLSs that are subject to failure.
Failures in the mechanical protection of SCs, as well as their material, can also occur due to wear over time or manufacturing imperfections, imperfections that may not have been detected upon acceptance of the SCs.

(*) Cyberattacks, the new reality that could contribute to changing the *status quo* in terms of digital security.
SCs can become targets for malicious actions. The physical security of SCs and related infrastructures has become a crucial variable in the equation for protecting global communications.
Purposeful attacks on SCs can occur in a pre-conflict situation (hybrid warfare) and will certainly occur in a war situation.
SCs are a military target in pre-conflict and conflict situations and have been for over 150 years!

2. CONTRIBUTION TO THE ELABORATION OF A NATIONAL STRATEGY

In a modest exercise of strategic reflection, 5 specific areas are identified where 25 recommendations can be considered to improve the resilience of SCs in Portugal. It should be noted that there are synergies to be obtained so that the "Whole will be greater than the simple sum of the Parts" and that these measures should be integrated into a national strategy that has as a national goal to strengthen the resilience of digital ecosystems, namely, in this specific aspect, on SCs.

a. System Redundancy through Diversification

To ensure continuity of service, it is important to have redundancy in communication systems. This can be achieved by landing additional SCs and establishing alternative routes that can be activated in case of failure of one or more SCs.

Recommendations:

1) Develop the diversification of routes, the diversification of SCs on the same route, the diversification of CLSs in national territory and also diversification in the terrestrial interconnection network of CLSs (backhaul).
2) Invest in the interconnection of national CLSs by domestic SCs (cabotage or *festoon*) in addition to the terrestrial interconnection network.

b. Monitorization and Supervision

The implementation of continuous monitoring and supervision systems can serve as prevention and can mitigate the impact and help to respond more quickly to any damage or interruption in SCs.

Recommendations:

3) Invest in sensing technologies of SCs allowing the detection of external impacts (SMART[1] Cables and in addition OFS[2] - DAS[3], SoP[4], Phase Interferometry, etc.) and support the integration of this data with the normal operational data of the SCs.

4) Promote the reinforcement of surveillance and adoption of increased protection measures, namely at critical points:
- near the landing of SCs, namely in the Dry Segment (shore end and the BMH and between the BMH and the CLS),
- and in the Wet Segment (shore end) and in critical areas of SC routes in shallow and deep waters.

5) Develop the implementation of advanced monitoring systems for real-time detection and analysis of anomalies or potential risks. AI algorithms can analyse large volumes of monitoring data to identify patterns and predict possible failures before they occur and can also be used to predict failures and optimize preventive maintenance. This centralized monitoring/supervision should be provided by a certified public entity, as a public service for monitoring and supervision of SCs in the EEZ and Territorial Waters through the establishment of a multi-layer platform that integrates monitoring data from various sources (AIS[5], RF, Radars, sensing, etc.). This proactive approach can significantly reduce response time to natural accidents (landslides, turbidity currents, earthquakes, etc.) or incidents due to human activity (whether intentional or not).

c. Physical Protection

Reinforcing the physical protection of SCs is essential for system security. This has been a concern for SC installers for a long time, but it deserves even greater attention may including route changes, the use of more resistant cable protective coatings that increase mechanical resistance to traction and impacts, and the installation of cables at greater depths, out of reach of natural accidents, but above out of reach of human activities that may cause damage. However, the creation of protection zones for SCs along their routes, being those exclusion zones for anchoring, fishing, dredging and deposition of materials, can significantly reduce the risk of damage to SCs, and this is where the difference will be made.

[1] https://www.smartcables.org/
[2] https://www.viavisolutions.com/en-us/resources/learning-center/what-fiber-optic-sensing
[3] https://www.ofsoptics.com/what-is-distributed-acoustic-sensing-das/
[4] https://www.science.org/doi/10.1126/science.abe6648
[5] https://en.wikipedia.org/wiki/Automatic_identification_system

Recommendations:

6) Prioritize the planning of maritime space by allocating areas dedicated to various activities (fishing, submarine power cables, telecommunications SCs, wind energy platforms, deep sea mining, emissaries and water collection pipelines for desalination and cooling, etc.), planning of this maritime space where protection and supervision zones for SCs will be established ("corridors" with pre-authorizations for partial Licensing and as protection zones for SCs), above all not identifying the routes of the SCs, knowing only that in these marked zones there may be SCs (not knowing how many, much less which ones).
7) Develop the promotion of the burial of SCs in shallow waters, promotion of the use of protective coatings for SCs on the shore end and HDD[6] practices near the coast.

d. Portugal Overview

In national terms, it will be important to develop initiatives that promote the involvement of various public and private stakeholders, in collaboration and cooperation, with coordination by authorities and public entities at various levels being necessary.

Recommendations:

8) Intensify didactic advice for the adoption of new security requirements in the SCs Licensing process that land in Portugal.
9) For the cases of SMART Cables that land in Portugal, give these cables priority and added speed in the Licensing processes as they bring added value to the country, since in addition to providing interconnection, they contribute with data from the Observation part to the protection of the cable itself (and other SCs in its vicinity) and serve science (climate change, oceanography, geophysics, etc.) and society (early warnings to the population of the arrival of earthquakes and tsunamis).
10) Legislate to ensure data sharing obligations for sensing obtained by SCs (SMART Cables and SCs with OFS) that cross our extended Exclusive Economic Zone (EEZ) and national territorial waters and that do not land in national territory.
11) Carry out inspection actions in the Dry and Wet Segments, as well as audits and periodic inspections in the CLSs and Dry Segments to guarantee compliance and performance.

[6] https://www.hadleeandbrunton.co.nz/what-is-horizontal-directional-drilling/

12) Facilitate the parking of cable ships in ports in the "CAM Zone" and the installation of SC spare parts warehouses near the respective ports to facilitate the logistical maneuverer of launching and repairing SCs.
13) Invest in facilitating the activity of SC installation/repair ships in territorial waters and the EEZ.
14) Carry out naval exercises to protect SCs in national waters involving the Armed Forces and other agents protecting critical infrastructure.
15) In close collaboration with CPEC (Communications Emergency Planning Committee), invest in promoting periodic SCs restoration exercises that land in Portugal with the necessary and essential involvement of Operators (with a very probable need to resort to terrestrial networks); such practice was common in Portugal before the liberalization of the sector in the 80s/90s and ceased to be practiced at the regional level from the beginning of this century, with very few examples of mutual aid agreements between international systems currently.
16) Develop national contingency plans to allow rapid and efficient responses to specific incidents that compromise the physical security of SCs (Wet and Dry Segment).
17) Promote the systematic carrying out of tests and exercises in Portuguese FTZs (Free Technological Zones) of new SC monitoring and repair techniques.
18) Promote collaboration between Operators and local communities in protection and monitoring initiatives.
19) Strengthen the technical training of SC repair teams (civilian and military) to guarantee a minimum national responsiveness in this area.
20) Promote the establishment of partnerships with the Navy, Authorities, Academia and the SC Industry (operators and suppliers) to create an R&D cluster with a view to innovation in technological development for the protection of SCs.

e. Internacional Cooperation

Collaboration between nations is crucial for the protection of SCs. Participation in international bodies and organizations is very important, and the creation of international agreements and protocols can facilitate the exchange of information with a view to greater readiness in response. Coordination of efforts is fundamental to protect this vital infrastructure of SCs. Portugal, due to its geostrategic location, can play an important role in promoting and leading global initiatives aimed at increasing the security of SCs.

Recommendations:

21) Invest in international cooperation (bilateral and multilateral) to strengthen the sharing of knowledge and resources utilization.

22) Adhesion of national stakeholders to the International Cable Protection Committee (ICPC)[7].
23) Strengthen our participation and collaboration with the North Atlantic Treaty Organization (NATO)[8] and the European Defence Agency (EDA)[9].
24) Strengthen the representation of the Portuguese State in the EU Agency for Network and Information Security (ENISA)[10] and in the International Telecommunication Union (ITU)[11] to address the security of SCs.
25) Promote the strengthening of bilateral and multilateral cooperation between National Authorities with competences and responsibilities for Security in telecommunications.

[7] https://www.iscpc.org/
[8] https://www.nato.int/nato-welcome/index_pt.html
[9] https://eda.europa.eu/
[10] https://www.google.com/search?client=firefox-b-d&q=enisa
[11] https://www.itu.int/en/Pages/default.aspx

Conclusion

Increasing the resilience of SCs in Portuguese waters is a multifaceted task with the intervention of many stakeholders from various sectors, but it is eminently a function of State sovereignty. The global dependence on SCs for secure and stable communications is very relevant, and ensuring the resilience of SCs as a critical infrastructure is becoming increasingly essential for the security and economic prosperity of Portugal and the world.

In our opinion, these 25 measures or recommendations articulated in 5 distinct, but interconnected areas constitute essential conditions for obtaining greater resilience of the digital system that constitutes the SCs network.

The assumption of the same will allow greater consistency, security and reliability in our domestic and international communications (regional and intercontinental) that use SCs, contributing to Portugal being able to constitute itself as an example in the global context of security of Submarine Cables.

Being the Portuguese Waters safe for SCs, this will facilitate the landing of new international SCs in the country, also contributing to Portugal becoming a Digital Hub in the Northeast Atlantic, according to the concept then developed during the Portuguese Presidency of the EU during 2021: *Portugal will not be an Island in the Digital Ocean*.

Lisbon, February 7, 2025

José Sousa Barros

Chair of Advisory Board of Observatory of Ecosystems and Digital Infrastructures

conselhoconsultivo@oeid.pt ; jose.barrosSCs@outlook.pt

Luís Manuel Brás Bernardino

President of Observatory of Ecosystems and Digital Infrastructures

presidente@oeid.pt

Web Page: https://oeid.pt/

LinkedIn Page: linkedin.com/in/oeidobservatório

ACRONYMS:

AI: *Artificial Intelligence*

AIS: *Automatic Identification System*

BMH: *Beach Manhole*

CAM: *Continent, Azores and Madeira*

CLSs: *Cable Landing Stations*

CPEC: *Communications Emergency Planning Committee*

CSs: *Telecom Submarine Cables*

DAS: *Distributed Acoustic Sensing*

EDA: *European Defence Agency*

EEZ: *Exclusive Economic Zone*

ENISA: *European Union Agency for Cybersecurity*

FTZs: *Free Technological Zones*

HDD: *Horizontal Directional Drilling*

ICPC: *International Cable Protection Committee*

NATO: *North Atlantic Treaty Organization*

OFS: *Optical Fibre Sensing*

R&D: *Research and Development*

RF: *Radiofrequency*

SMART: *Scientific Monitoring and Reliable Telecommunications*

SoP: *State of Polarization*

UIT: *International Telecommunication Union*