# Best practices for protection and resilience of submarine cables.

## Global Network Architecture Group (GNA-G)

**Brazilian Committee for the Protection of Submarine Cables**
CBPC

# 1 The value of the ocean to a nation.

# The value of the ocean to a nation.

**The value of territorial waters is assessed by countries using four parameters:**

1) **Source of resources** ⇨ Fishing, oil exploration, tourism, etc…

2) **Means of transport** ⇨ Cargo transport.

3) **Strategic domain** ⇨ Control over the EEZ (Exclusive Economic Zone) allows other countries to use or not use this space as they see fit.

*4)* ***Exchange of information*** ⇨ Originally ships carrying mail, then telegraph cables, and today through submarine cables.

# The importance of submarine cables

“Submarine cables are critical infrastructure, carrying approximately **more than 15 trillion dollars in daily transactions.”**

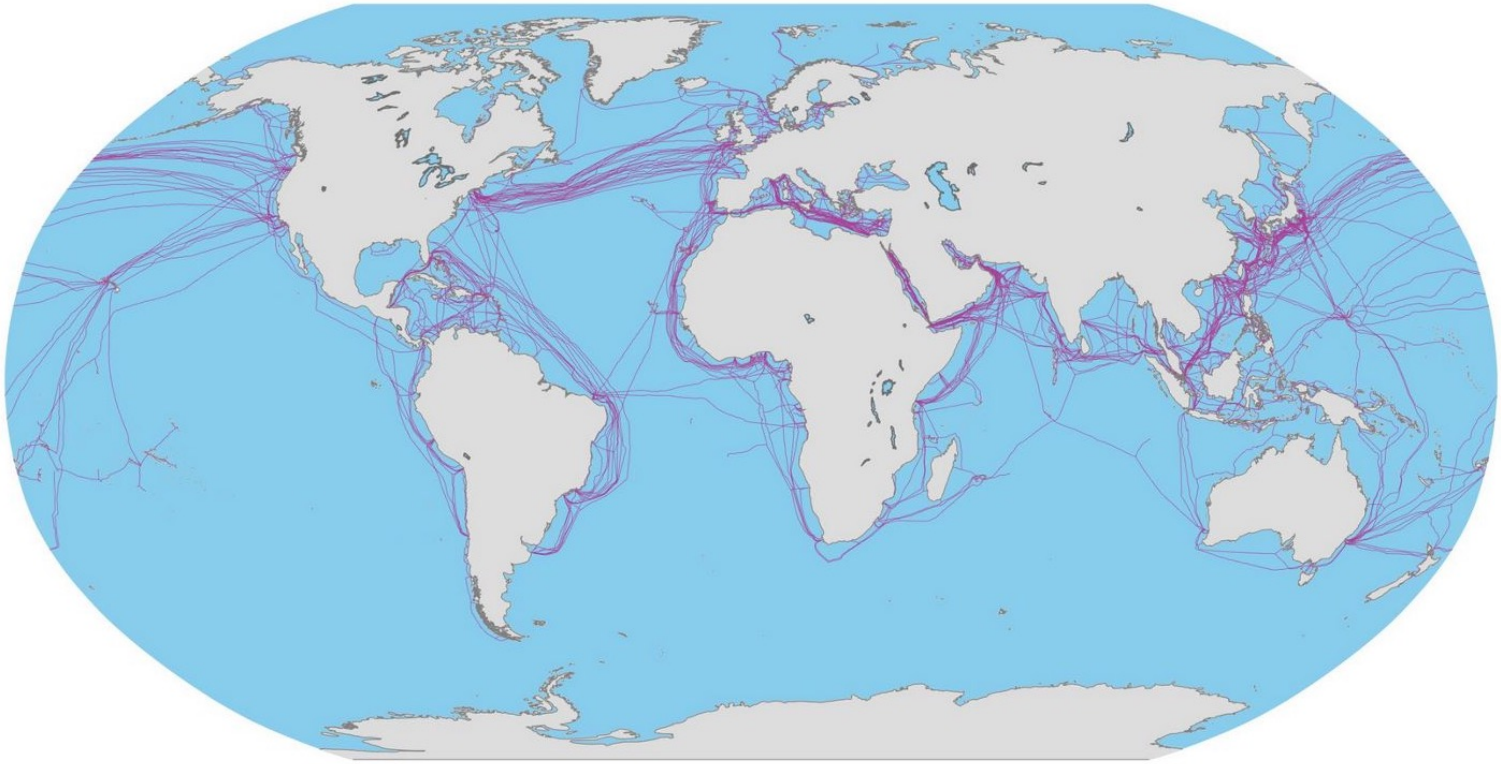
“When a submarine cable reaches a country, it is usually followed by many companies with multinational operations; typically, **that country's GDP increases by 2% or 3% in the following years.”**

“**Submarine cables today are responsible for 98% of global data, voice, and video traffic**, with more than 172 years of history.”

“This is a subject that **encompasses many technologies**: information science, nonlinear optics, electrical engineering, materials engineering, engineering practices, project management, maritime expertise, high reliability standards, and complex business.”

# The global network of submarine cables

Today in the world, there are **over 600 cable systems and 1,500 CLSs (landing points)** that are currently active or under construction.



# 2 Governing principles

## Government action in protecting and ensuring the resilience of submarine cables.

- **Focus on statistically significant risks** where government action could have the greatest impact on risk reduction.

- Promote commercial and regulatory environments that **encourage multiple and diverse connections** of domestic and foreign submarine cables.

- **Promote transparent regulatory regimes** that expedite cable deployment and repair according to well-established timelines.

- **Consult with the industry to understand** technology and operational parameters and to share risk data.

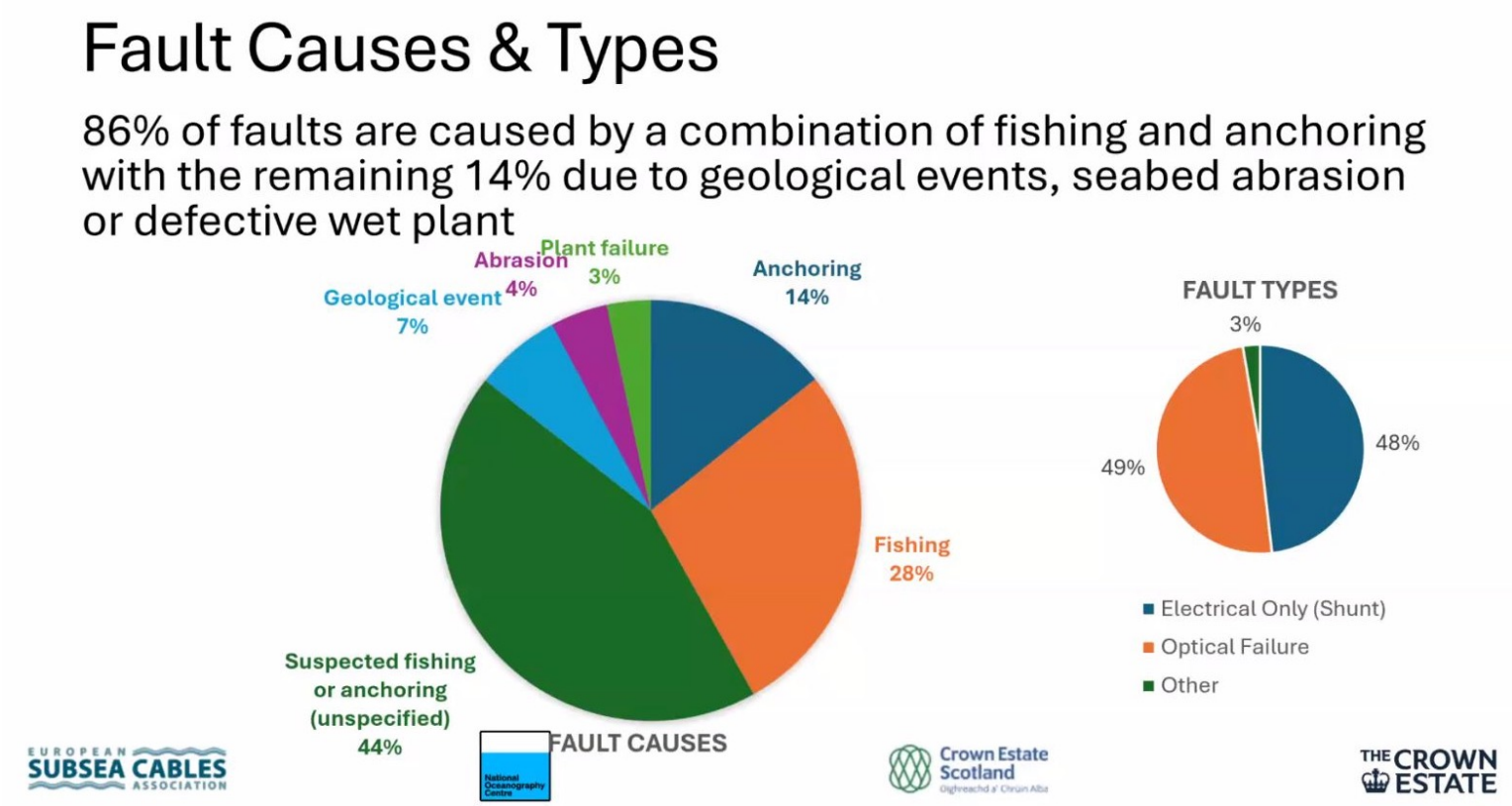
- **Complement existing industry best practices.**

- **Promote freedoms on the high seas** to encourage submarine cable deployment and repair.

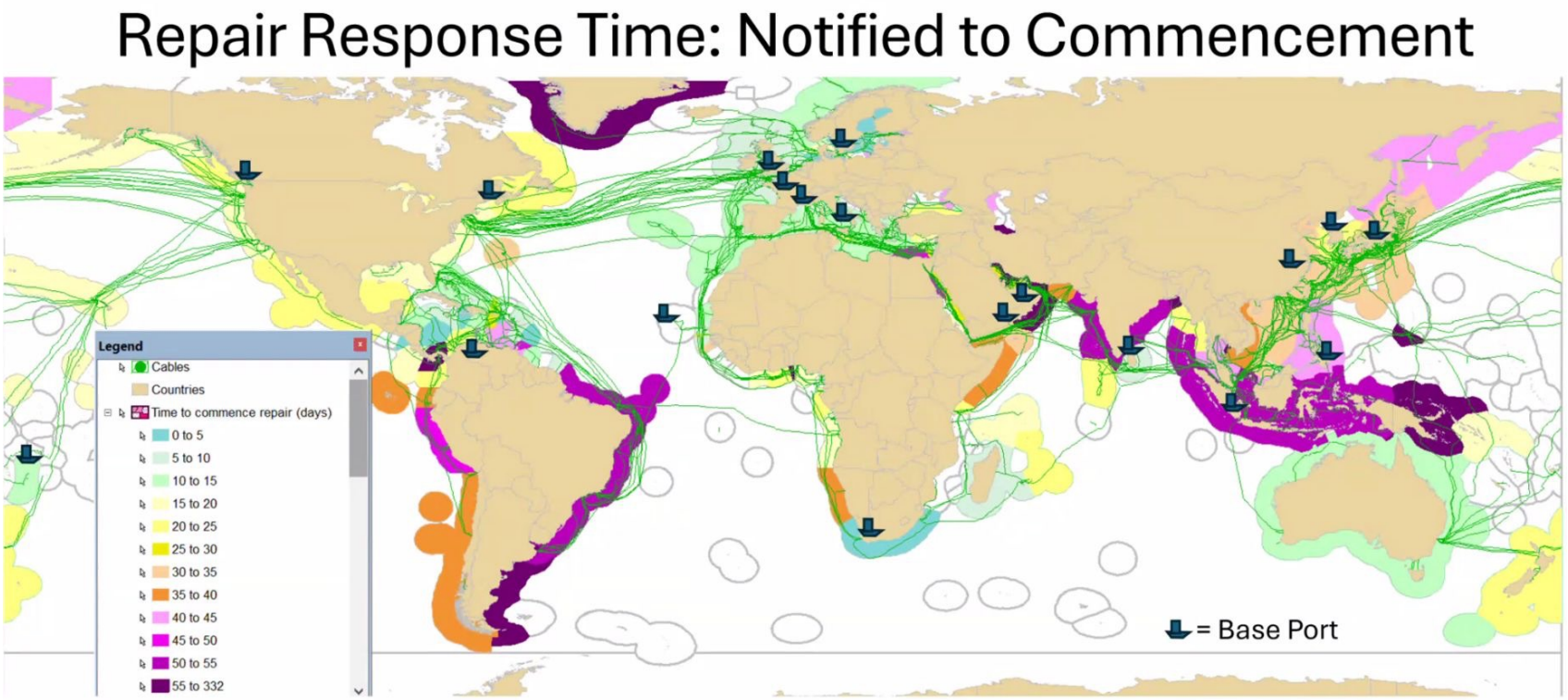
- **Engage with other states on a global and regional basis,** as the actions of other states can significantly affect the connectivity of an individual state.


# 3 Risks and threats

# Risks and threats to submarine cables



# Risks and threats to submarine cables



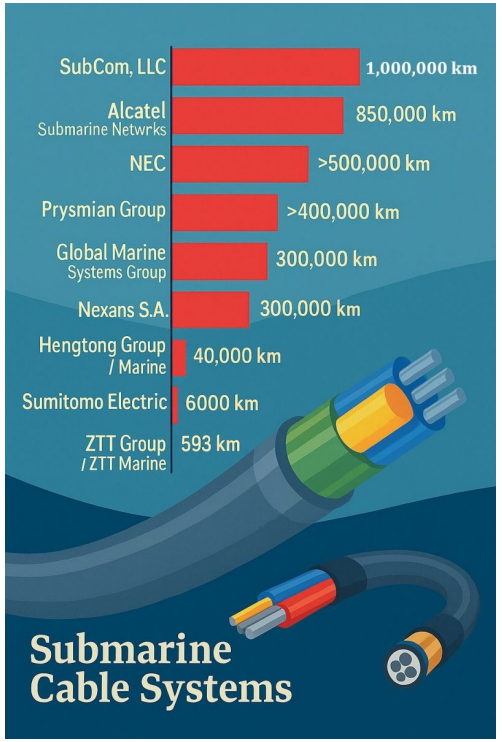

Cable database source: GMSL Geocable. Maritime Boundaries source: General Dynamics GMDB

# The Integrity of Submarine Cables – Repair Costs

High Estimates of Costs in Fiber Optic Submarine Cables

| Causes | % Share | Faults per Year | Avg Cost / Fault | Total Cost |
|---|---|---|---|---|
| Fishing/Anchoring | 57% | 17 | $3 million | $51 million |
| Deliberate Sabotage | 9% | 3 | $3 million | $9 million |
| Natural Events | 5% | 1.5 | $3 million | $4.5 million |
| Shoreline Erosion | 5% | 1.5 | $3 million | $4.5 million |
| Component Failure | 6% | 2 | $3 million | $6 million |
| Unknown | 18% | 5 | $3 million | $15 million |
| Total | 100% | 30 | $80 million | $90 million |

Latam Region



# The costs of cuts for the industry and the country

In 2024, there were 214 submarine cable breaks worldwide. Let's analyze what this means in terms of economic losses for telecommunications operators and the damage in a country like Brazil:

When a cable is cut, it takes 10 to 40 days from fault detection to full service restoration, not considering misuse of the repair process. Overall, let's consider an average of 25 days.

Fault detection (1 to 23 days), vessel mobilization (2 to 10 days), on-site repair (5 to 15 days), obtaining licenses and coordination (up to 15 days), and delays due to weather and other factors (up to 10 days).

# The costs of cuts for the industry and the country

These are the operational and financial costs faced by the consortium of operators whose cable was cut:

- Repair vessel: **up to US$100,000 per day (US$500,000 to US$2 million per incident);**
- Materials for cable repair: **(US$200,000 to US$1 million);**
- Compensation for SLA violations for companies and OTTs: **US$100,000 to US$10 million;**
- Purchase of temporary bandwidth on alternative routes: **US$50,000 to US$5 million;**
- Loss of revenue: **US$100,000 to US$5 million.**

**Therefore, we are talking about US$1 million to over US$10 million for a consortium per incident.**

# The costs of cuts for the industry and the country

Thus, considering a 25-day downtime, we are talking about US$40,000 to US$400,000 per day.

Assuming 10 operators in the consortium, the cost would be approximately US$10,000 to US$100,000 per operator per day.

While this may seem enormous, it is minuscule compared to the loss per incident for the country where the interruption occurs.

The estimated national loss due to slow internet, banking and cloud services, as well as losses in stock exchanges and financial institutions, is approximately US$100 million per day on average, ranging from US$36 million to US$300 million per day.

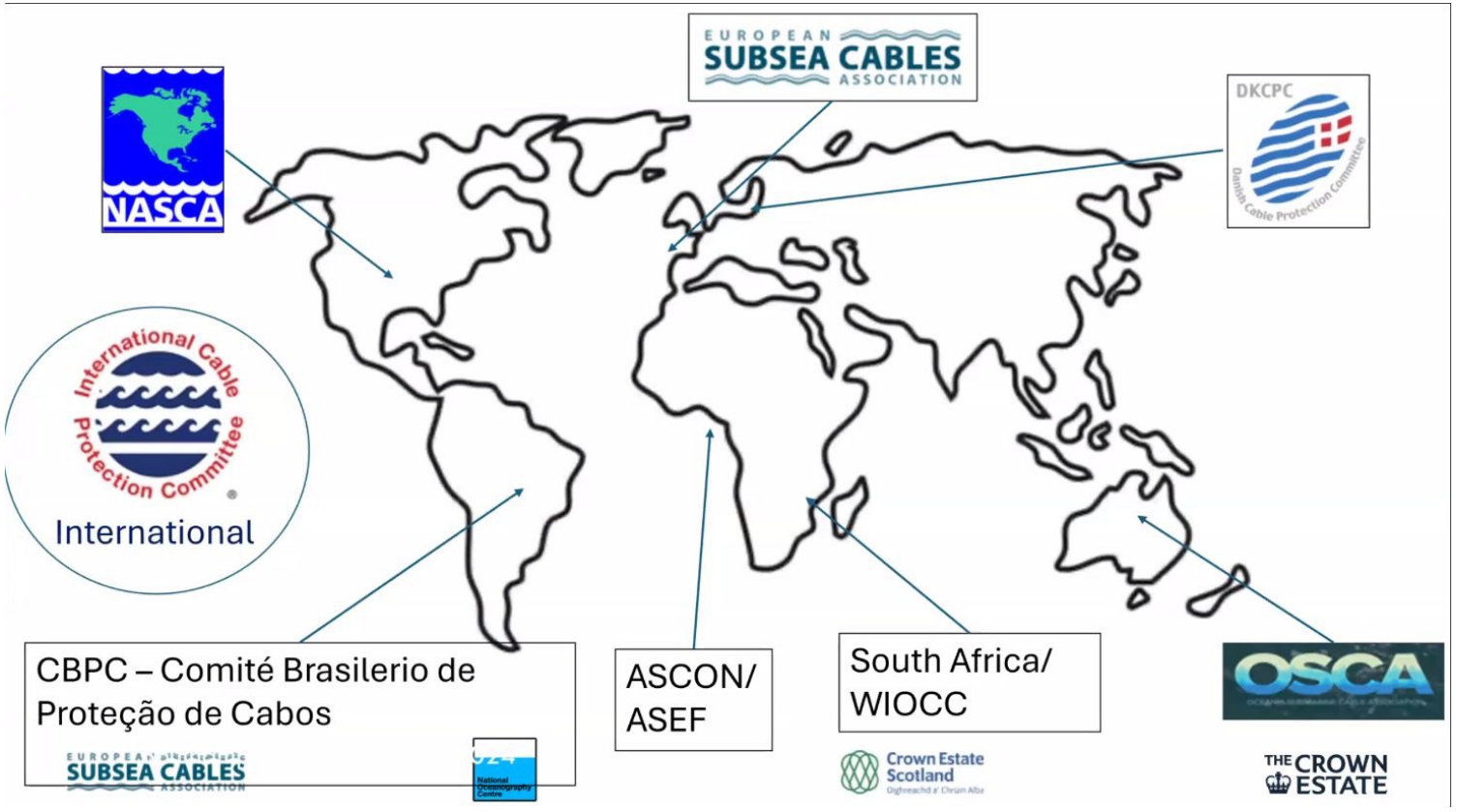
**Assuming a 25-day outage, each incident costs countries an average of US$2.5 billion and up to US$7.5 billion per outage in extreme cases.**

For 214 incidents, we are talking about a GDP loss of more than half a trillion dollars per year worldwide.

# 4

# *CBPC – Brazilian Committee for the Protection of Submarine Cables*

# Brazilian Committee for the Protection of Submarine Cables



# Brazilian Committee for the Protection of Submarine Cables

The main objectives of the CBPC:

a) To recommend approaches for the spatial separation of submarine cables and other offshore activities/infrastructure to ensure infrastructure protection and communication continuity.

b) To examine gaps, conflicts, and sources of delay in existing federal, state, and local inter-institutional coordination for offshore licensing and recommend mechanisms to improve coordination without increasing regulatory burdens.

c) To address industry best practices and government policies to promote the geographic diversity of submarine cable routes and landings by identifying risks to submarine cable infrastructure, both natural and artificial, and possible protection measures used to mitigate such risks.

# 5 Relevant themes and topics at CBPC 2026/2027

# Relevant themes and topics at CBPC 2026/2027

- Encourage and/or require the use of AIS by smaller vessels.
- Guide the Coast Guard to issue warnings to mariners about submarine cables and to communicate with vessels operating or navigating near submarine cables or in the process of coastal shipping.
- Encourage operators to adopt Sea-Risk type systems.
- Cooperate with neighboring nations regarding illegal, unreported and unregulated fishing.
- Create Cable Protection Zones and Corridors.
- Pre-license repair vessels.
- Provide technical support for the new Brazilian submarine cable law (PL-270/2025).
- Conduct awareness-raising activities with fishing communities.
- Work with the government on the framework for the removal and recycling of legacy submarine cables.

# 6 Operation Trident (Brazilian Navy)

# Submarine Cable Protection Exercise

# Operation Trident (Brazilian Navy) - Submarine Cable Protection Exercise

- Operation Trident was an exercise developed by the Brazilian Navy with the participation of the Brazilian Committee for the Protection of Submarine Cables, carried out in November 2025.

- During three days of intense activity at sea, Operation Trident placed military personnel and specialists before a highly realistic scenario: the detection and neutralization of a Multi-Role Ocean Surveillance (MROS) vessel attempting to cut a strategic submarine cable. From there, the coordination between the submarine S-41 Humaitá (Scorpene Class), SH-16 Seahawk aircraft, and maritime patrol aircraft, as well as frigates, ROVs, and cyber command centers, highlighted the level of complexity involved in defending assets that support the functioning of the country.

- The result was clear: protecting submarine cables demands technology, readiness, and interoperability.

- The protection of critical submarine infrastructure proved to be an extremely difficult operation, even for forces equipped with modern means. Operation Trident demonstrated that locating an underwater cable—even with nautical charts, known coordinates, and advanced sensors—can take days of searching. In the exercise, it took two days to find a cable located approximately 40 nautical miles from the coast and 100 meters deep, using all available resources. This result makes it clear that a malicious actor would need expensive, bulky, and specialized resources to attempt real sabotage.

# Operation Trident (Brazilian Navy) - Submarine Cable Protection Exercise

- The use of the K120 NSS Guillobel, simulated as an MROS-profile vessel capable of launching ROVs and operating advanced sensors, highlighted the need for multi-source tracking capabilities. Simultaneously, the S-41 Humaitá submarine demonstrated the efficiency of collecting acoustic signatures from ROVs, revealing the relevance of submarine warfare for cable protection. The SH-16 Seahawk aircraft, launching sonobuoys, provided acoustic redundancy, while the P-95 Bandeirante enhanced visual and electromagnetic reconnaissance. The scenario demonstrated that the defense of these assets depends on a complex fusion of data between surface, subsurface, aviation, and cybersecurity modules.

- Operation Trident was not limited to the military environment: it involved, in an unprecedented way, representatives from the federal government, states, municipalities, **Brazilian Cable Protection Committe** and some of the country's main telecommunications and digital infrastructure companies, such as Azion, Claro Brasil, V.tal, Angola Cables, Telxius, Sparkle, Cirion, EllaLink, Google, Seaborn, Petrobras Oil Company, NIC.br, and Anatel. The exercise reinforced the perception that submarine cables support not only the internet, but also banking, logistics, port, hospital, and public security systems.

- The specialized civilians who participated in the operation worked alongside the Armed Forces, strengthening interoperability between IT and OT networks, security APIs, and incident response structures. This cooperation model represents exactly the architecture that would be necessary in a real crisis. Furthermore, the disclosure of Operation Tridente broadened the defense culture in the country, demonstrating to society that protecting these cables guarantees everything from financial transactions to the continuity of essential services. The operation reaffirms that digital and physical security are now inseparable domains.

# Operation Trident (Brazilian Navy) - Submarine Cable Protection Exercise

- TThe most important lesson was unequivocal: yes, sabotage at sea is possible, but operationally very complex, slow, expensive, and detectable. A malicious agent would need a large ship with an MROS profile, ROVs, sonar, sensors, a specialized crew, prior knowledge of the cable routes, and prolonged time in the area. The strategic conclusion is clear: the best defense is resilience, with route diversification, physical and logical redundancy, and expansion of maritime surveillance capabilities. Operation Tridente points the way: Brazil is capable of protecting its assets, but must continue to evolve to face an increasingly contested maritime environment.

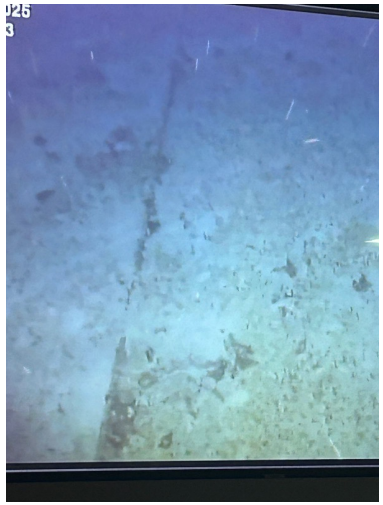
- **In other words, can we talk about sabotage at sea? Yes, but it is something very, very complex to carry out. Investing in resilience and diverse pathways is the best way to mitigate this kind of thing.**

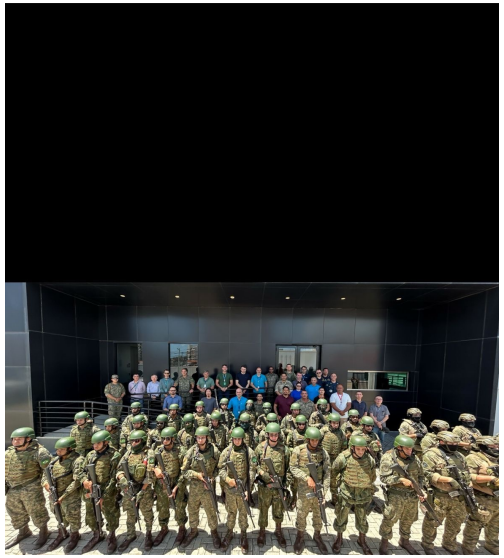
# Operation Trident (Brazilian Navy) - Submarine Cable Protection Exercise




Rogério Mariano – CBPC – February 2026

# Operation Trident (Brazilian Navy) - Submarine Cable Protection Exercise






# 7 Final recommendations from CBPC

# Final recommendations from CBPC

Establish clear lines of communication between all stakeholders involved in a cable, i.e., the various state agencies with regulatory capacity and security functions in the countries connected to the cable, as well as the industries involved in its installation, operation, and maintenance.

Common systems and protocols exist for information sharing among security agencies responsible for cable protection, enabling them to identify suspicious activities and respond quickly to incidents.

Enhanced maritime surveillance to attribute any incident to a vessel and potential perpetrators.

Agreements and transparency on how the international law of the sea (including the UNCLOS and IMO conventions) is interpreted in cable protection.

Investments in cable resilience and repair.

Common understandings on who pays for what in cable protection (consumers, taxpayers, or shareholders).

Strategic signaling and deterrence against any adversaries who have declared an intention to damage cable connections in peacetime deliberately.


# Doubts?

https://www.linkedin.com/in/rogerio-mariano-065a1340/

rogerio.mariano@azion.com


you're
Rad
Merci
GRACIAS
Thank
You
Danke
Sag
Olun
MADE MY DAY
THANKS
A
BUNCH