

Enhancing the Resilience of Submarine Internet Infrastructure



An Internet Society Public Policy Brief

November 2025

Executive Summary

As dependence on digital services intensifies, the resilience and security of submarine cable systems are increasingly under scrutiny—particularly in light of recent outages in Africa, Tonga, and South Asia. While geopolitical tensions and hostile threats receive much attention, most cable disruptions—around 200 per year¹—are the result of natural causes or human error.

This brief draws on real-time insights from the Internet Society’s Pulse platform and the European Union’s 2025 Action Plan on Submarine Cable Security to highlight the current risks, emerging best practices, and tools for improving resilience. Drawing from examples in Bangladesh, the Pacific Islands, and Europe, it explores how regional cooperation and transparency can ensure that submarine infrastructure remains robust, redundant, and inclusive.

This document offers a forward-looking, optimistic approach to strengthening Internet resilience through practical and policy-driven solutions. Recommendations emphasize improved mapping, diverse connectivity routes, and public-private collaboration to protect the infrastructures we can no longer afford to ignore.

Introduction

Beneath the waves lies an invisible network that keeps the world connected: submarine cables. Individual private companies and consortia of companies own and operate a network of more than 500 commercial undersea fibre-optic cables—570 as of 2025, with another 81 planned²—that carry 97-98%³

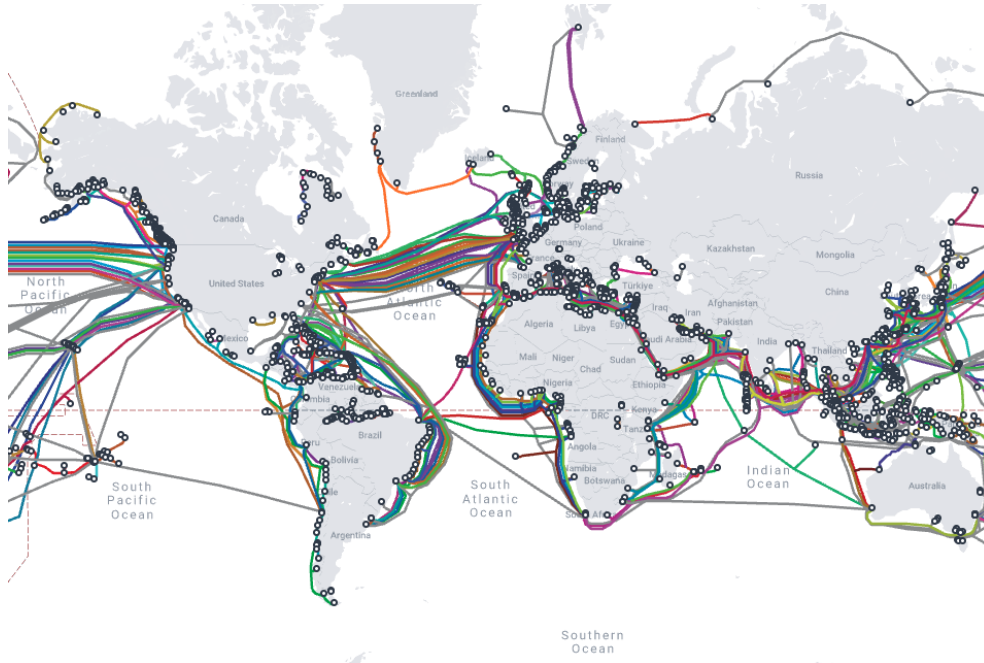
¹ Is It Sabotage? Unraveling the Mystery of Undersea Cable Breaks, TeleGeography, Feb 2025 - <https://blog.telegeography.com/is-it-sabotage-unraveling-the-mystery-of-undersea-cable-breaks>.

² How Many Submarine Cables Are There, Anyway?, TeleGeography, Feb 2025 - <https://blog.telegeography.com/how-many-submarine-cables-are-there-anyway>

³ Subsea telecommunication cables are essential for Europe’s digital connectivity, Nov 2024 <https://digital-strategy.ec.europa.eu/en/library/subsea-telecommunication-cables-are-essential-europes-digital-connectivity>



of the world's intercontinental Internet traffic, forming the backbone of global communications, finance, education, and security. And yet, for all their importance, submarine cables rarely command public attention until they suffer a failure. When they do, on some occasions, the disruption is beyond mere inconvenience—it may have a temporary impact on economies and access to information flows.



Source: TeleGeography <https://www.submarinecablemap.com/>, under the [Creative Commons License: Attribution-ShareAlike 4.0 International \(CC BY-SA 4.0\)](#).

Submarine infrastructure, by its nature, is both vital and vulnerable. Its remoteness, exposure to natural elements, and dependence on a limited number of landing points pose inherent risks. However, vulnerability does not imply helplessness. Around the world, policymakers and network operators are beginning to treat submarine infrastructure with the urgency it deserves. This policy brief explores the significance of these cables, examines global responses to recent outages, and proposes concrete actions to safeguard connectivity in an increasingly digital world. The key concept of this policy brief is resilience, which is not about avoiding failure but about preparing for it.

The Internet Society acknowledges the work of the International Cable Protection Committee⁴ (ICPC), founded in 1958. Together with the International Advisory Body for Submarine Cable Resilience⁵, established by the International Telecommunications Union in 2024, they are key global organizations that help identify potential ways and means to improve the resilience of this vital infrastructure that powers global communications and the digital economy.

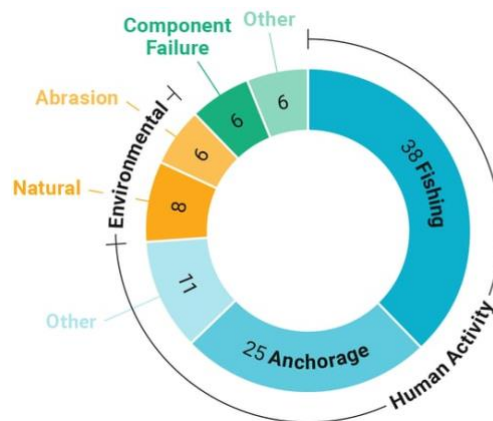
⁴ The International Cable Protection Committee <https://www.iscpc.org/>

⁵ The International Advisory Body for Submarine Cable Resilience <https://www.itu.int/digital-resilience/submarine-cables/advisory-body/>

The Infrastructural Backbone Few Think About

While they receive a great deal more attention by the popular press, satellites play only a minor role in global Internet connectivity. Submarine cables remain the primary channel for high-capacity, low-latency international data transmission. These cables, often no thicker than a garden hose, crisscross the ocean floors, linking continents and countries. Their efficiency and cost-effectiveness are unmatched.

However, their invisibility contributes to their neglect. In March 2024, multiple cable cuts off the coast of West Africa caused massive service disruptions in Côte d'Ivoire, Liberia, Ghana, and other countries. As shown in real-time by the Internet Society's Pulse Platform, latency—the time it takes for data to travel between sender and receiver—surged, and availability plummeted across the region⁶. The outage revealed a harsh truth: without cable diversity and supporting terrestrial infrastructure, even a single undersea event can leave millions without reliable access.



Cause of faults of submarine cables (%). Source: TeleGeography

Another important factor is the availability of vessels and personnel to repair broken cables. The waiting time can be substantial, due to logistical scheduling of vessels as well as the distance to travel⁷. Building dedicated regional repair fleets to ensure swift response and repair of damaged cables can be an essential way to reduce the impacts of damaged cables.

Learning from Resilience: The Bangladesh Case

But there are also encouraging stories. Bangladesh, struck by a submarine cable outage in 2023, was able to maintain Internet services by rerouting traffic through terrestrial connections with India and

⁶ 2024 East Africa Submarine Cable Outage Report July 2024, <https://www.internetsociety.org/resources/doc/2024/2024-east-africa-submarine-cable-outage-report/>

⁷ Strengthening Taiwan's Critical Digital Lifeline, Charles Mok and Kenny Huang, August 2024, <https://fsi.stanford.edu/publication/strengthening-taiwans-critical-digital-lifeline>

relying on locally cached content.⁸ This experience illustrates that resilience⁹ is not about avoiding failure, but about preparing for it.

Bangladesh's ability to weather the storm was no accident. Its investments in regional interconnection, content distribution, and redundancy paid off. In contrast, countries with limited domestic hosting and no land-based backup connections were left struggling.

Analysis¹⁰ from the Internet Society's Pulse platform underscores that countries scoring higher on infrastructure diversity—measured through metrics like transit provider diversity and number of IXPs—tend to experience less severe impacts and faster recovery during submarine cable outages; as the West Africa case shows, countries with multiple transit providers experienced less severe disruptions.

Other alternatives that may serve as hybrid backup systems in case of failures, are satellite communications and portable communication units¹¹, which can provide quick connectivity solutions until the submarine infrastructure is repaired.

Europe Takes Notice: The 2025 EU Action Plan

Governments are increasingly recognizing the importance of submarine infrastructure, not just from a security lens but from a resilience standpoint. The European Union's 2025 Joint Communication on Cable Security¹² lays out a comprehensive response. Unlike the *reactive* measures of some regions, the EU has adopted a preventative, cross-sectoral approach that emphasizes cross-border coordination, better monitoring, and the need to address both geopolitical risks and everyday hazards such as seismic activity or accidents related to fishing activity.

What's notable about the EU plan is its dual approach that acknowledges the potential threats while also emphasizing the need for responsible infrastructure growth. It urges member states and private operators to map infrastructure more transparently, strengthen operational coordination, and invest in public-private partnerships. This recognition of submarine cables as critical infrastructure represents an important step forward in resilience policymaking.

⁸ Bangladesh Coping With Submarine Cable Outage Thanks to Indian Terrestrial Cables, Local Content Caches, April 2024, <https://pulse.internetsociety.org/blog/bangladesh-coping-with-submarine-cable-outage-thanks-to-indian-terrestrial-cables-local-content-caches>

⁹ To know more about resilience, please visit <https://pulse.internetsociety.org/en/resilience/>

¹⁰ Don't put all your Internet infrastructure in one basket, October 2023, <https://pulse.internetsociety.org/blog/dont-put-all-your-internet-infrastructure-in-one-basket>

¹¹ New technology to help communities stay connected following disasters, Government of New South Wales, September 2024, <https://www.nsw.gov.au/media-releases/new-technology-to-help-communities-stay-connected-following-disasters>

¹² EU Action Plan on Cable Security, February 2025, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0009>

Shifting from Reaction to Prevention

Too often, Internet infrastructure policy reacts to failures instead of preventing them. But that tide is beginning to turn. Around the world, initiatives are emerging that blend technical foresight with local empowerment. In the Pacific, regional hubs are being developed¹³ to host content closer to users, reducing reliance on distant cables. In landlocked countries like Zambia, targeted investment in local IXPs and partnerships with neighboring countries are closing the connectivity gap¹⁴.

A crucial innovation enabling this shift is the development of common standards for the description of fibre optic infrastructure deployments and norms regarding information sharing. The Open Fibre Data Standard¹⁵ (OFDS) is a great example of this with regard to terrestrial fibre optic networks. Championed by the Internet Society, OFDS establishes a common language and transparency around fibre-optic infrastructure deployments. The result is better-informed planning, quicker responses to failures, and smarter resource allocation. There is a similar need for transparency norms and descriptive language regarding undersea fibre optic cables.

The Open Fibre Data Standard (OFDS) has been developed in collaboration with the World Bank, International Telecommunication Union, Mozilla Corporation, Liquid Intelligent Technologies, CSquared, and Digital Council Africa.

As an open data, open standard initiative, the OFDS facilitates the exchange, analysis, and visualization of fibre network data across different stakeholders, including governments, telecom providers, and researchers. By providing a consistent schema (a standardized structure for organizing data), it enhances interoperability, transparency, and informed decision-making in broadband expansion efforts.

OFDS describes what data to publish about fibre optic networks, and how to structure and format data for publication and use. It does so through a set of common concepts and definitions about what fibre network data should contain and how it should be structured. The standard also contains guidance and tooling to support the publication and use of fibre network data in a range of formats to suit most user needs.

¹³ Pacific's Connectivity Hub. Region's Content Capital?, December 2024, <https://pulse.internetsociety.org/blog/pacifics-connectivity-hub-regions-content-capital>

¹⁴ How Does Zambia Accelerate its Internet Resilience, September 2024, <https://pulse.internetsociety.org/blog/how-does-zambia-accelerate-its-internet-resilience>

¹⁵ The Open Fibre Data Standard, April 2025, <https://www.internetsociety.org/blog/2025/04/the-open-fibre-data-standard/>

Building Resilience: Policy Principles for the Future

Resilience is not a destination but a continuous process. It requires not just cables and routers but strategies and partnerships. Based on global evidence and insights from Internet Society's Pulse¹⁶ research, the following principles are key:

First, invest in infrastructure **diversity**. Relying on a single route—especially a single submarine cable—is a recipe for disruption. Whether through additional submarine paths or terrestrial links, redundancy must be built into national networks.

Second, promote data **openness and transparency**. Open standards like OFDS allow all stakeholders—governments, ISPs, and civil society—to make smarter decisions. They reduce duplication, highlight risks, and promote accountability. Transit offers should inform about redundancy and security measures.

Third, **decentralize** Internet infrastructure. Distribute content, by hosting it locally and deploying off-net caching servers to reduce latency, keep traffic inside borders, and lessen dependence on fragile international connections.

Fourth, foster regional **collaboration**. As the Lisbon SubOptic conference¹⁷ emphasized, resilience cannot be achieved in isolation. Governments and network operators must work across borders to share intelligence, build trust, and coordinate responses.

Finally, define Internet **preparedness** as a national policy objective. That means tracking performance, setting goals, and adapting strategies in real time. Internet Society's Pulse measurement tools provide a foundation, but commitment must come from policymakers.

Fibre optic infrastructure plays an increasingly important role as the backbone of Internet traffic around the world. Understanding the interplay and interconnection of these fibre optic backbones is essential to developing a more complete picture of Internet resilience.

Conclusion: Toward a More Resilient Digital Future

Submarine cables may be vulnerable, but they are not undefendable. Most breaks occur not from espionage or sabotage, but from accidental cuts, natural disasters, or aging equipment. While these risks can't be eliminated, their impact can be mitigated.

¹⁶ Internet Society Pulse: <https://pulse.internetsociety.org/>

¹⁷ Takeaways From Lisbon SubOptic 2025, July 2025, <https://pulse.internetsociety.org/blog/takeaways-from-lisbon-suboptic-2025>

The tools are available: open standards, smart infrastructure investment, and informed policy. What's needed is alignment. Resilience is not just about surviving the next outage—it's about building a digital ecosystem that can adapt, recover, and thrive.

The moment to act is *now*. As Internet usage accelerates and geopolitical uncertainties rise, building resilient, transparent, and diversified submarine infrastructure is not just a technical necessity—it is a strategic imperative for global stability and economic prosperity.