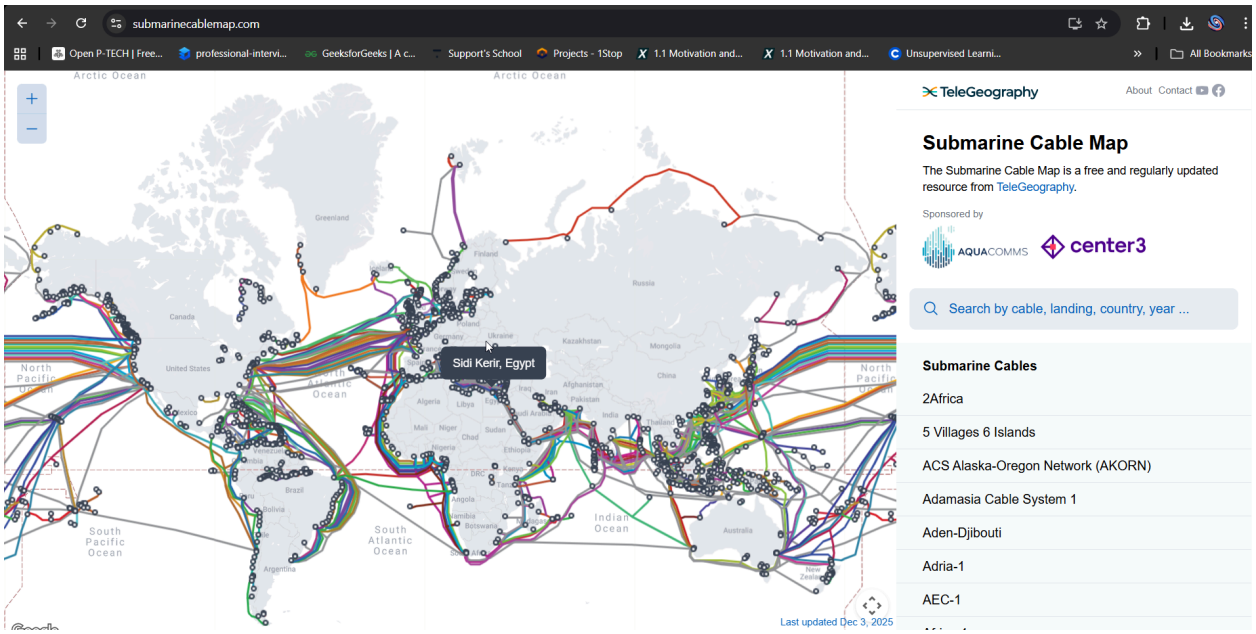
Submarine cables form the physical foundation of the global internet, carrying 95–99% of international data traffic across oceans.
On Day 8, I discovered this hidden infrastructure; on Day 9, I went deeper into how fragile it is — especially when geopolitics, sabotage suspicions, and accidental damage come into play. Together, these two insights reveal that the “cloud” is not floating in the sky — it rests on thin glass fibers lying on the seabed, and any disruption to them can instantly turn digital problems into very real-world crises affecting banking, communication, emergency services, and even criminal investigations.

Importance:
- The vast majority of global internet traffic physically travels through ~570–600 submarine cables spanning over 1.4 million kilometers.
- While most damage is accidental (fishing, anchors, earthquakes), deliberate or suspected sabotage in geopolitically tense areas is increasingly documented.
- A single major cable cut — or worse, coordinated damage to several — can isolate countries, severely slow international connectivity, and create cascading effects across critical sectors.
- This physical vulnerability means cybersecurity is no longer just about code: protecting undersea infrastructure has become a core national security priority.

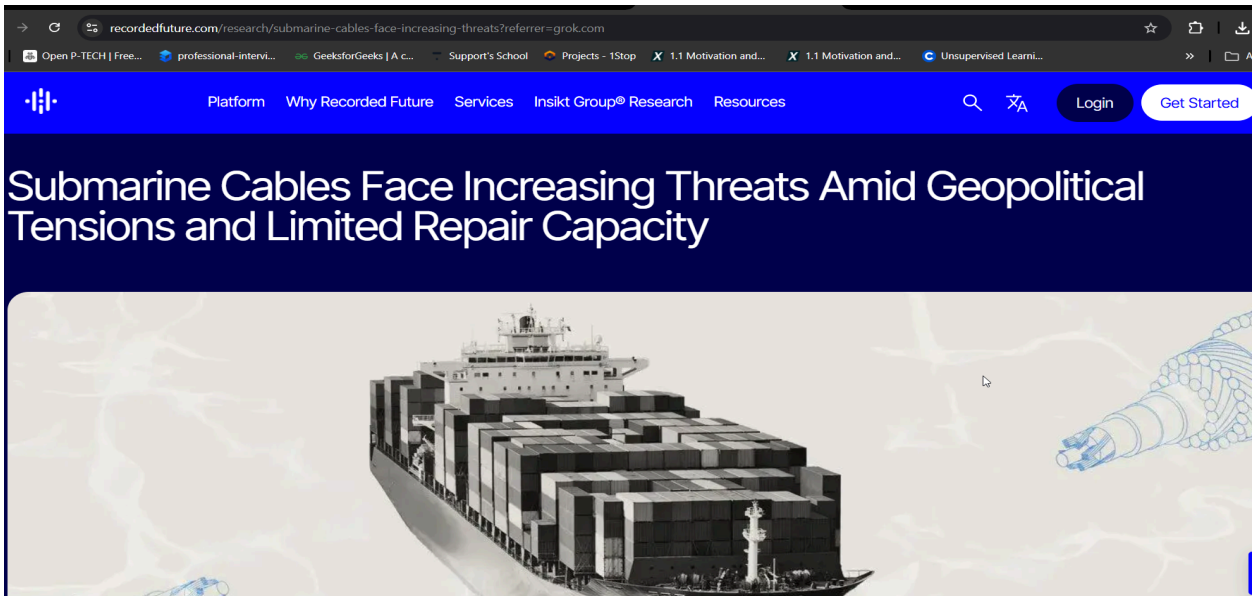


Why this matters in practice
A cyber attacker doesn’t necessarily need to breach a bank’s firewall — cutting the right undersea cables can achieve a massive denial-of-service effect across entire economies, often with plausible deniability. This physical-digital intersection is one of the most important (and under-discussed) realities of modern security.

Divider

The Physical Backbone of the Digital World: Submarine Cables, Their Critical Role, and Rising Vulnerabilities (January 2026 Comprehensive Overview)

The internet most people experience feels instantaneous, wireless, and intangible. Yet beneath the surface — literally — lies a network of submarine fiber-optic cables that carries the overwhelming majority of international data traffic. These cables are the arteries of globalization: they enable everything from Zoom calls between New York and Tokyo, stock trades between London and Hong Kong, remittances from the U.S. to the Philippines, to secure military and diplomatic communications.



Core Facts About Submarine Cable Infrastructure (2025–2026)

- **Number of active/planned systems:** Approximately 570–597 commercial submarine cable systems (TeleGeography 2025–2026 data).
- **Total length:** More than 1.4 million kilometers — enough to circle the Earth 35+ times.
- **Traffic carried:** 95–99% of intercontinental internet traffic (Internet Society 2025 policy brief; multiple industry sources consistently place satellite contribution at 1–5% or less).
- **Ownership trend:** Hyperscalers (Google, Meta, Microsoft, Amazon) now co-own or fully control a growing share — estimated 40+ systems by late 2026 — reflecting the strategic importance of direct, high-capacity links.

How the System Normally Works

Modern submarine cables use advanced dense wavelength division multiplexing (DWDM) technology, allowing a single pair of fibers to carry hundreds of terabits per second. Cables are laid in protected seabed corridors, armored near shorelines, and buried in shallow waters. Redundancy is built in: most routes have multiple parallel or alternative cables, so a single cut usually causes temporary slowdown rather than total blackout — except in regions with limited diversity.

The Reality of Vulnerability: Types of Threats

Threat Type	Approximate Share of Incidents	Typical Cause	Impact Severity	Examples (2024–2025)
Accidental damage	70–80%	Fishing trawlers, ship anchors	Usually moderate (rerouting possible)	Routine global faults (~200 per year)
Natural events	10–15%	Earthquakes, underwater landslides, volcanic activity	Varies — can be severe in low-redundancy areas	Tonga 2022 eruption, West Africa rockslides
Suspected deliberate interference	Rising but still minority	Anchor-dragging by suspicious vessels, possible state-linked activity	Potentially very high (coordinated cuts)	Baltic Sea (8–11 incidents), Taiwan waters (5–11)

Major Geopolitical Hotspots (2024–2025)

- Baltic Sea — At least 8–11 confirmed cable damages between late 2024 and December 2025. Several incidents involved vessels suspected of deliberate anchor-dragging (some linked to Russia or opaque ownership). Affected countries: Sweden, Finland, Germany, Baltic states. Consequences included disrupted banking transfers, telecom outages, and temporary loss of secure government communications.
- Waters around Taiwan — 5–11 documented incidents during heightened China-Taiwan tensions and military drills. Disruptions ranged from domestic connectivity to international links, raising serious concerns about gray-zone coercion tactics.
- Red Sea — February 2024 Houthi-related damage affected multiple Asia-Europe cables, slowing global traffic by 10–20% on affected routes.
- West Africa / South Africa — Multiple natural and dragging incidents caused prolonged outages in Nigeria, Ghana, South Africa, and neighbors — severely impacting mobile money services, remittances, and government operations.

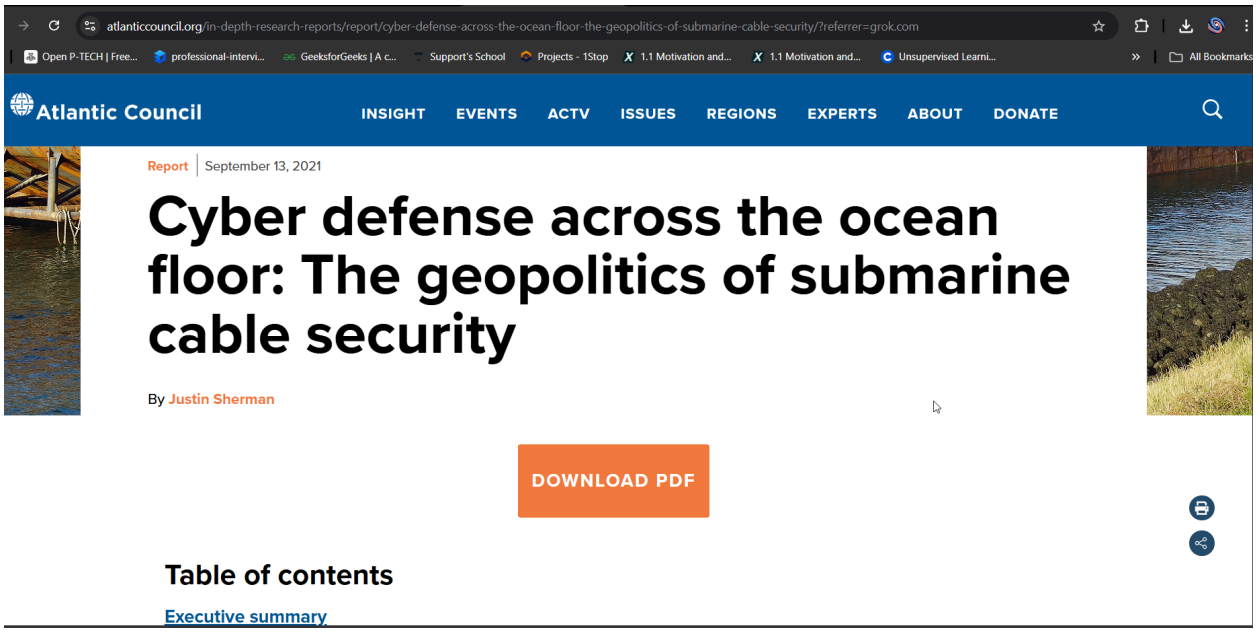
Real-World Sector Impacts
When multiple cables are cut or when redundancy is limited, effects cascade quickly:

- Banking & Finance — International wire transfers fail, stock exchanges experience latency, ATMs and mobile banking become unreliable.
- Communication — Cloud services, VoIP, email, video calls, and social media slow dramatically or become unusable.

- Emergency & Government Services — 911-equivalent systems, police coordination, disaster response, and secure diplomatic/military links suffer.
- Criminal Investigations — Real-time surveillance feeds, access to cloud-stored evidence, and international data-sharing channels are interrupted — sometimes for days or weeks.

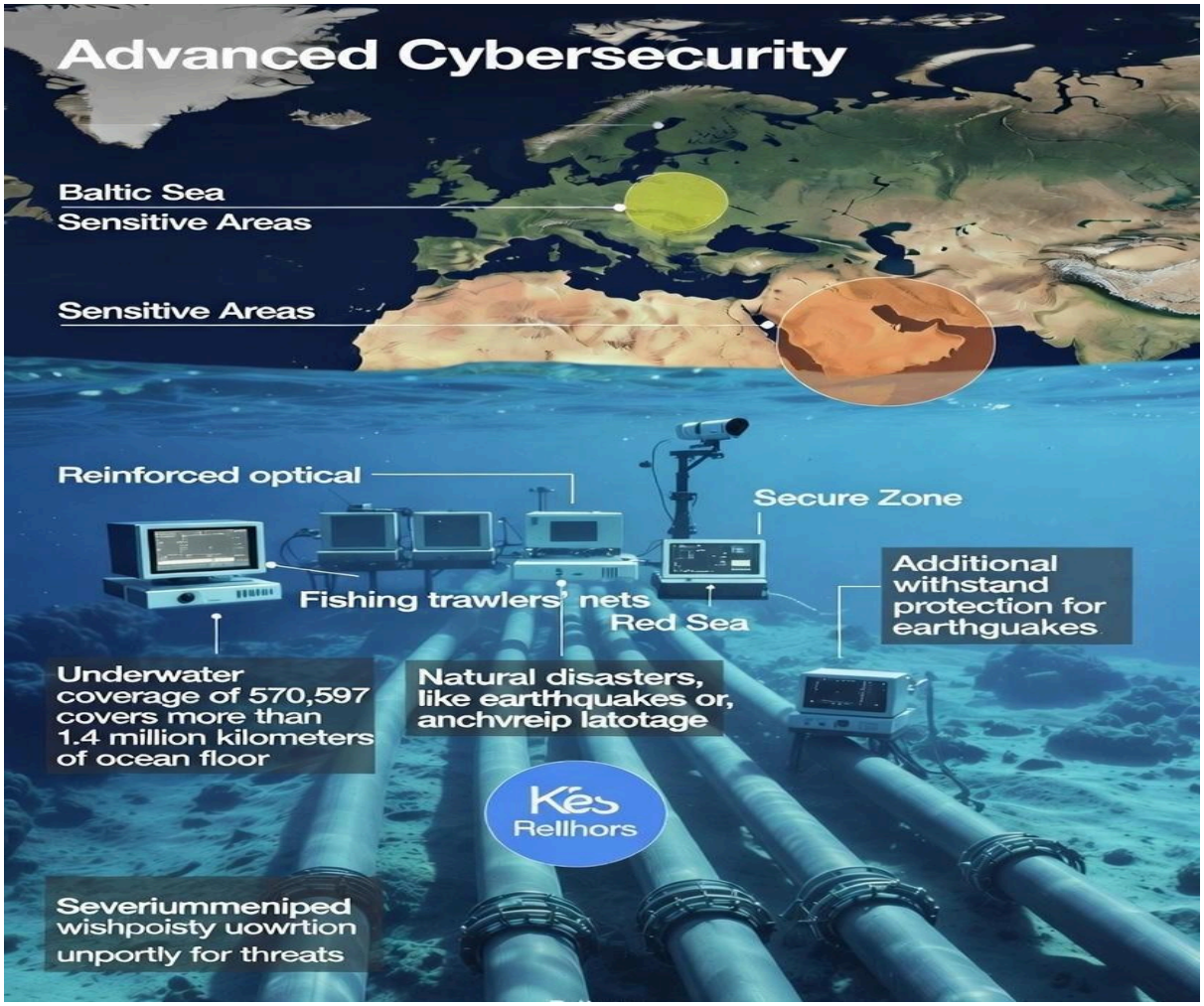
The Emerging Physical-Digital Security Paradigm
Experts increasingly describe submarine cables as a new domain of hybrid warfare. A coordinated physical attack on cables can deliver effects comparable to the most sophisticated cyber campaign — without needing to penetrate a single firewall. State actors (or their proxies) can exploit this with plausible deniability, especially in regions where attribution is difficult.

This has triggered several responses:
- Increased investment in cable diversity and new routes
- Push for faster repair capabilities (more cable ships, pre-positioned spares)
- Classification of landing stations as critical infrastructure
- Heightened physical and cyber protection around cable endpoints
- Diplomatic efforts to establish norms around cable protection (though enforcement remains challenging)



Current Snapshot (January 2026) stats:

Metric	Value	Source
Active submarine cable systems	570–597	TeleGeography 2025–2026
Total length	>1.4 million km	TeleGeography
Intercontinental traffic share	95–99%	Internet Society 2025 policy brief
Annual cable faults	~200 (mostly accidental)	Submarine Cable Almanac / industry reports
Countries with ≤2 international cables	~40 (highest vulnerability)	ITU / TeleGeography
Repair time (typical)	2 weeks to several months	Industry estimates



Final Insight
Combining Day 8's realization (the internet physically travels under oceans) with Day 9's deeper dive (how easily that physical layer can be disrupted) creates a much clearer picture: the digital world rests on remarkably thin, vulnerable glass strands on the seabed. Protecting this infrastructure — from accidental damage to deliberate sabotage — is no longer a niche concern. It is a fundamental requirement for global economic stability, national security, and the continued functioning of modern society.

Key Citations(sources):
https://www.submarinecablemap.com/ (TeleGeography interactive map)
https://www.internetsociety.org/resources/policybriefs/2025/enhancing-the-resilience-of-submarine-internet-infrastructure/
https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats
https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/
https://blog.telegeography.com/2025-submarine-cable-map
https://www.visualcapitalist.com/submarine-cables/
https://en.wikipedia.org/wiki/Submarine_communications_cable
https://www.reuters.com/technology/baltic-sea-cable-cuts-raise-sabotage-fears-2025-01-02/
https://www.ft.com/content/8f2b3c1a-4d2e-4e9b-9c0d-2e1f5a7b8e3a (Financial Times coverage of Taiwan-related incidents)