Securing Global Communications:
An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure

Joint hearing before the
U.S. House of Representatives Committee on Homeland Security

Subcommittee on Transportation and Maritime Security and the
Subcommittee on Cybersecurity and Infrastructure Protection

November 20, 2025

Opening Statement of Tim Stronge

Chairmen, Ranking Members, and distinguished members of the committee. Thank you for the opportunity to speak with you today.

My name is Tim Stronge, and I am the Chief Research Officer at TeleGeography. We provide the independent data that the global communications industry relies on to map and measure the internet.

I am here today to talk about the physical backbone of the modern U.S. economy: submarine fiber-optic cables. The strategic importance of this network boils down to three characteristics: these cables are **vulnerable**, they are **critical**, and they are **irreplaceable**.

First, **vulnerability**. I've brought a cable sample with me. Encased inside are thin strands of glass, each about the width of a human hair.

If this looks fragile to you, that's because it is. Individual cables are especially vulnerable to damage from fishing gear and anchor drags. The global network experiences roughly 200 faults every year—an average of four per week.

Second, **criticality**. My son Kaz is away at college in Connecticut. One of our favorite ways to stay connected is to share funny videos. Fiber-optic networks make that possible. Perhaps you already lay awake at night, worrying about how we must protect our nation's strategic reserve of cat videos. But even if not, it's important to understand that cables carry far more than social media and web content.

They are the backbone of global finance. More than $12 trillion in financial transactions flow over these cables *each day*. Millions of American jobs now depend on access to digital infrastructure. The U.S. government, itself, is heavily reliant on commercial submarine cables.

Third, **irreplaceability**. A common misconception is that satellites are a viable one-for-one replacement. They are not. Satellites are a vital *emergency backup* for mission-essential use, but they cannot replace the sheer capacity and cost-efficiency of fiber. Cables carry over 99% of all intercontinental data for a simple reason: the cost-per-unit of cable capacity is 2,800 times cheaper than satellites.

Collectively, these three conditions—physical vulnerability, high criticality and irreplaceability—might seem like a scary mix.

But I am here today with good news. For a cable operator, the loss of revenue streams during downtime is financially catastrophic. That means that these private companies are already powerfully self-incentivized to secure their cables.

Let's return to that vulnerability. The vast majority of those 200 annual faults are *accidents*. This constant threat has compelled the private sector to invest billions of dollars in a tangible, layered defense.

Companies have built dozens of new cables and geographically diverse landing stations to ensure data always has a backup path. Cable operators are innovating with new detection technology that uses the fiber itself to sense threats. And they have funded a global fleet of two dozen repair vessels on 24/7 standby.

Crucially, the strategies built to defend against routine accidents will also help to secure the network against malicious attacks.

However, there are critical gaps where government action is needed:

1. **First, designate a single point of contact for cables.** The existing inter-agency permitting process can be confusing and painfully slow. The industry needs one specific federal lead to shepherd new cable projects.

2. **Second, strengthen deterrence.** Current penalties for damage to cables date back to an 1884 treaty on *telegraph* cables and are woefully—almost comically—insufficient.

3. **Third, help fast-track cable repair abroad.** The global average delay to *begin* a repair is now a month and a half. Much of that is due to complex permitting in foreign waters. We need a diplomatic push to cut the foreign red tape keeping repair ships in port.

The industry has already demonstrated its deep commitment to cable security. It looks to government as a partner to help clear the path.

Thank you, and I look forward to your questions.

TeleGeography

Securing Global Communications:

An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure

Hearing before the
U.S. House of Representatives
Committee on Homeland Security

Subcommittee on Transportation and Maritime Security and the Subcommittee on Cybersecurity and Infrastructure Protection

November 20, 2025

Written Testimony
Tim Stronge

Table of Contents

Executive Summary

Submarine fiber-optic cables are the critical, vulnerable, and irreplaceable backbone of the U.S. economy and national security, carrying over 99% of all intercontinental data and more than $12 trillion in daily financial transactions. Satellites, while vital, cannot replace this network.

This network is also inherently vulnerable. It experiences, on average, four faults per week worldwide, overwhelmingly from accidental human activity. The strategies industry has developed to defend against these routine accidents will also serve to secure the network against malicious attacks.

Industry-Led Resilience

A central finding of this report is that the private sector is already powerfully self-incentivized to ensure network resilience. This private investment is not theoretical. It is demonstrated by:

- **Proactive Diversity:** Investing billions in dozens of upcoming cables and new, geographically separate cable routes to eliminate single points of failure.

- **Physical Protection:** Voluntarily absorbing the high cost of deeper cable burial, which accounts for 60% of installation expense on just 12% of the global network.

- **Rapid Deployment:** Funding a 62-vessel global repair fleet and well-practiced maintenance procedures that a 2025 U.K. Parliamentary report called “efficient, well tested and robust.”

Public-Private Partnership

To maintain its leadership as the global data hub—a position built by private investment but now facing a more competitive, geographically diverse market—the U.S. must actively foster the public-private partnership that created this strategic asset.

Key policy considerations include:

- **Assign** a central federal authority to shepherd cable installation and repair through lengthy permitting rules that discourage investment.

- **Modernize** the woefully outdated 1884 penalties for cable damage.

- **Use diplomatic channels** to reduce repair permitting delays in foreign waters.

- **Avoid new mandates**, such as U.S. flag-only requirements for repair ships, which would cripple repair capacity.

The Role of Submarine Fiber-Optic Cables

While largely invisible, a network of submarine fiber-optic cables forms the indispensable backbone of the modern world. These systems are the primary conduit for the global economy, carrying over 99% of all intercontinental data. This entire global network, which has no viable technological replacement, is built from individual cables that are, by their physical nature, vulnerable to damage.

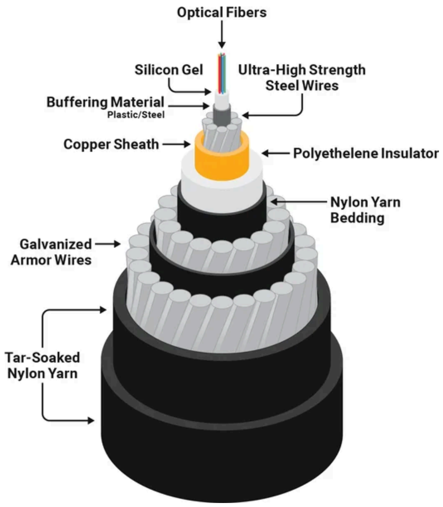
How Cables Work

Modern submarine cables use fiber-optic technology. Lasers on one end fire billions of times per second down thin glass fibers to receptors at the other end of the cable. These glass fibers are wrapped in layers of metal and plastic. Near shore ends, the cables are often wrapped in additional steel wire for protection.

For most of its journey across the ocean, a cable is typically as wide as a garden hose. The fiber-optic filaments that carry light signals are extremely thin — roughly the diameter of a human hair.

Cable landing stations (CLSs) function as the critical interface between submarine cable systems and a nation's domestic data infrastructure. These secure facilities, typically located near the coast, are responsible for processing the international data and feeding it into the terrestrial network.

Cross Section of a Submarine Cable with Optional Armoring



Installation

Specialized surface vessels lay cables directly on the ocean floor. Nearer to the shore, cables are often buried 1 to 3 meters (about 3 to 10 feet) under the seabed for protection. Considerable care is taken to ensure cables follow the safest path to avoid areas of heavy human activity such as fishing zones and anchoring areas. Cables also avoid geologic dangers such as steep inclines, geothermal vents, and fault zones.

Repair

Repairing a submarine cable is a complex, multi-day operation that takes place entirely on a specialized repair vessel. First, the vessel's operator must secure the necessary permits to conduct the repair. Next, the ship sails to the fault location, which is determined by tests from the land-based stations. To begin the repair, the ship often uses a specialized grappling hook ("grapnel") to find and lift the cable. Even if the cable is only damaged and not fully severed, it is typically cut in two on the seabed to bring each end to the surface. Once aboard, technicians in a sterile jointing room must splice in a new, additional section of spare cable to patch the two halves together, a process that involves individually fusing each microscopic glass fiber. After extensive testing, the cable is carefully lowered back to the seabed. If it was in a shallow, buried area, a remotely operated vehicle (ROV) may be sent down to re-bury it using high-pressure water jets.

Cable Deployments

The global submarine cable landscape currently consists of 596 in-service systems. While 112 new cables are officially planned and announced, our internal tracking suggests the pipeline is even more robust; TeleGeography is monitoring dozens of additional projects in various planning stages that are not yet public.

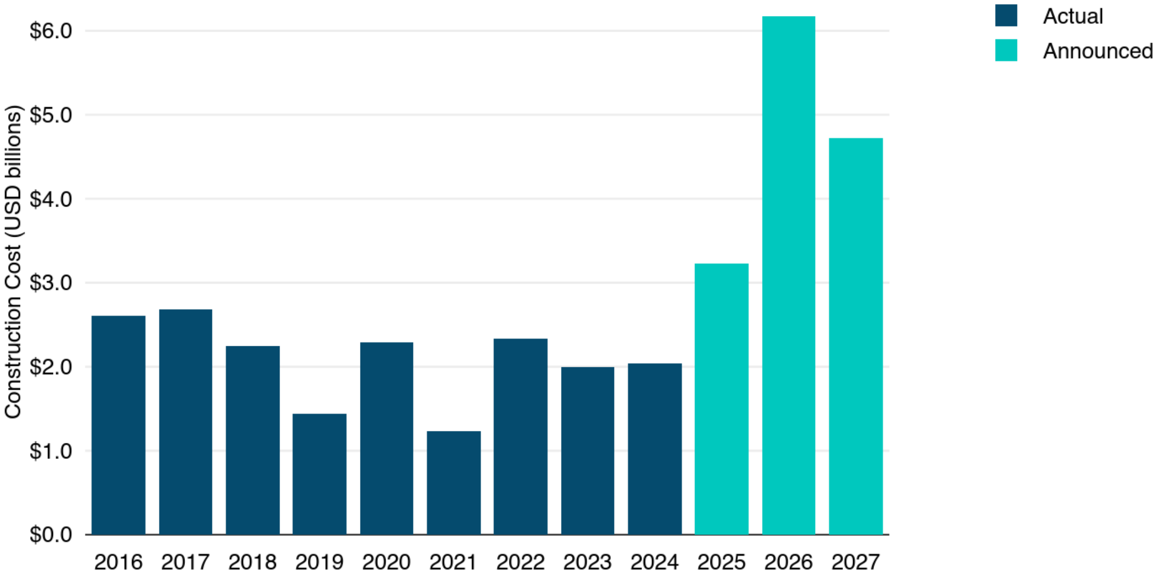
The United States currently has 96 active cables landing on its shores. What's even more telling is the future pipeline: the 34 new cables planned for the U.S. represent nearly a third of all publicly announced projects worldwide, underscoring America's critical importance as a global data hub.

To keep up with burgeoning demand, the industry is pumping billions of dollars of capital into new cable construction. Investment in new submarine cables has surged in recent years. Despite some fluctuations, new cable investment has averaged over $2 billion per year in the past nine years. TeleGeography forecasts that the value of new submarine cables entering service from 2025-2027 will reach over $14 billion.

Financing cables is a difficult task. In particular, regulatory/permitting delays introduce a lot of risk. Some of the cables currently slated for completion in the 2025-2027 period will likely slip by 1-3 years. Others may fail to finalize financing entirely and have their plans mothballed. Nevertheless, we anticipate that cable investment will remain at or near an all-time high.

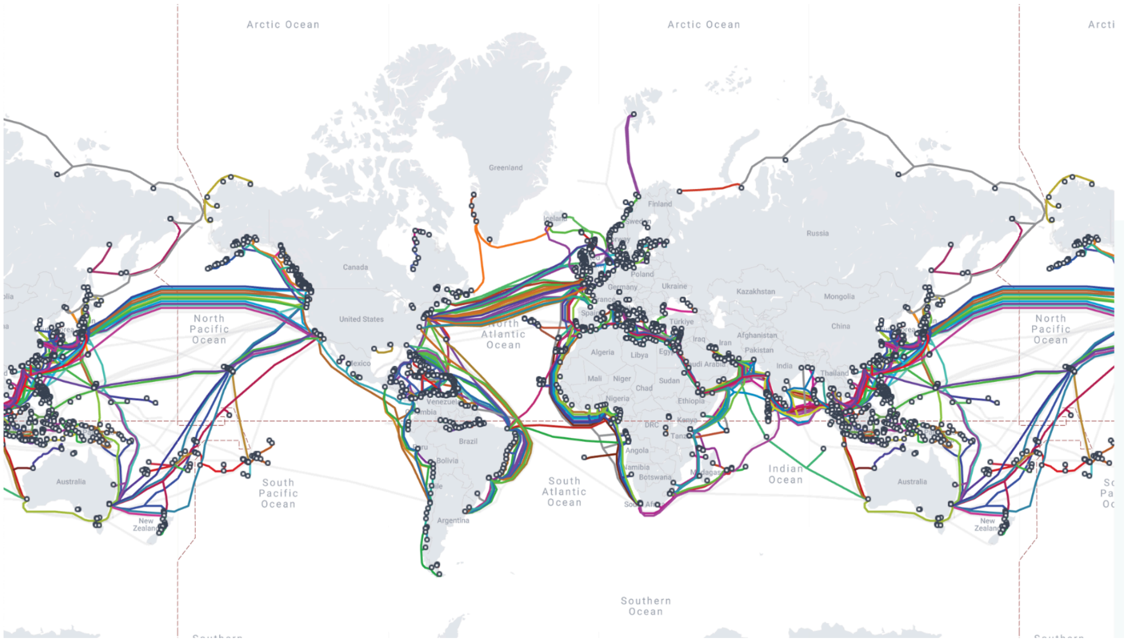
The charts and maps below illustrate the pattern of cable investments.

Combined Construction Costs of Cables Entering Service



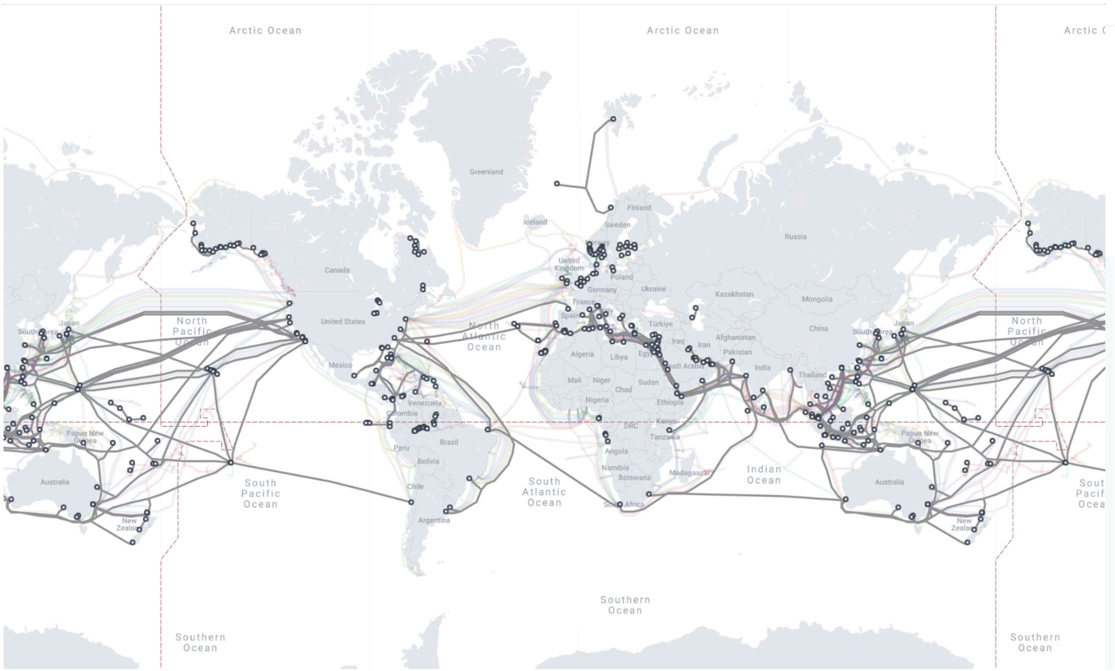
Notes: Total construction costs of all international and domestic submarine cables entering service in designated years. Construction costs exclude the cost of subsequent capacity upgrades and annual operational costs. 2025-2027 construction costs based on announced contract values and TeleGeography estimates. Not all planned cables may be constructed.
Source: TeleGeography's Transport Networks Research

Existing Submarine Cables



Source: TeleGeography (submarinecablemap.com)

Planned Submarine Cables



Source: TeleGeography (submarinecablemap.com)

Cable Usage and Ownership

Cables are generally built, owned, and maintained by private entities. Direct public investment in the cable industry is rare.

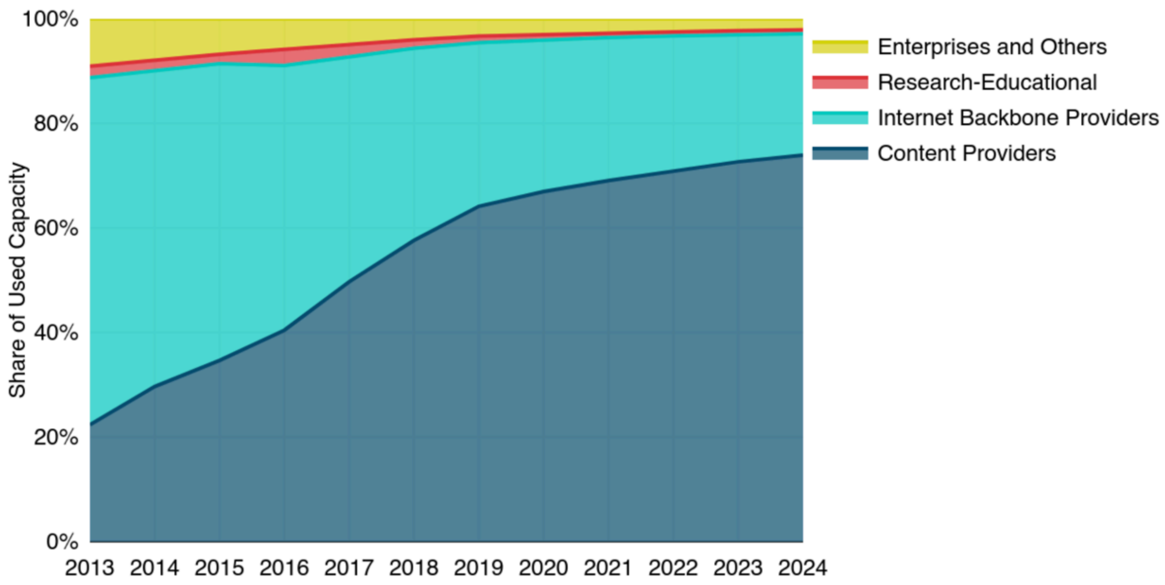
Cables were traditionally owned by telecom carriers who would form a consortium of all parties interested in using the cable. In the late 1990s, an influx of entrepreneurial companies built many private cables and sold off the capacity to users.

Both the consortium and private cable models still exist today, but one of the biggest changes in the past few years is the type of companies involved in building cables.

U.S. content providers such as Google, Meta, Microsoft, and Amazon are major investors in new cables worldwide. The amount of capacity deployed by private network operators, like these content providers (sometimes referred to as "hyperscalers"), has outpaced internet backbone operators in recent years. Faced with the prospect of ongoing massive internal network demand growth, directly owning new submarine cables makes sense for these companies. As the figure below shows, a large majority (74%) of the world's international telecom capacity is used by just a handful of content providers.

This private investment often follows a model analogous to a condominium, where the content provider acts as an anchor tenant. They sell or swap spare fiber pairs to other users, such as ISPs and carriers, a practice that has broadly subsidized and fueled the recent boom in new cable builds, lifting the capacity for all users.

Used International Bandwidth by Source



Source: TeleGeography's Transport Networks Research

Characteristics of Submarine Cables

The strategic importance of submarine cables can be understood through three core characteristics: their criticality, their vulnerability, and their irreplaceability.

Criticality

Undersea fiber-optic cables are critical infrastructure. While many of us associate the internet with personal connections—like sharing videos with family—cables are the foundation of the modern economy. Millions of American jobs now rely on access to digital infrastructure. Cables carry the vast majority of data for AI, cloud computing, and essential business communications. Furthermore, they are the backbone of global finance; our research confirmed that central banks rely on these cables to transmit a staggering $12 trillion in financial transactions daily. When a volcanic eruption severed the cable to Tonga, the nation's ATMs stopped working, demonstrating a direct link to financial stability. The U.S. government is itself heavily reliant on this commercial infrastructure for its own operations.

Vulnerability

Submarine cables are vulnerable. Despite their critical role, they are not fortress-like. A typical deep-sea cable is only the diameter of a garden hose. If this seems fragile, it is because, in many ways, it is. Faults are common; the global network experiences failures, on average, four times per week, primarily from the accidental human activity that will be detailed later in this report. While cables are armored and buried near shore, this partial protection is not a total guarantee, nor is it feasible to apply across the entire ocean.

Irreplaceability

Finally, no other communications technology on the horizon can replace undersea cables. A common misconception is that satellites can serve as a viable alternative. This is not the case. Satellites provide a vital emergency backup for mission-essential applications, but they cannot replace the sheer capacity and cost-efficiency of fiber. Cables carry over 99% of all intercontinental data for a reason: the cost-per-unit of data is estimated to be 2,800 times cheaper than via satellite. For the foreseeable future, there is no technological replacement for the submarine cable network.

Collectively, these three conditions—high criticality, inherent vulnerability, and total irreplaceability—might seem to present a dire security challenge. However, there are significant reasons for optimism. A variety of strategic options are available to protect this infrastructure, and the private sector has already invested billions of dollars to implement them with proven success.

Strategies for Protecting Cables

Overview

An effective national strategy for submarine cable security relies on a public-private partnership built around five core imperatives—a partnership that leverages the private sector's existing investments and leadership.

1. **Denial**: Ensuring that bad actors do not gain access to critical infrastructure.
2. **Diversity**: Ensuring data can be rerouted through multiple different cable paths.
3. **Detection**: Using monitoring systems to quickly identify and locate cable faults or threats.
4. **Deterrence**: Preventing damage from both hostile and accidental acts through clear regulations, legal accountability, and direct industry collaboration.
5. **Deployment**: Maintaining and rapidly mobilizing a robust cable repair capability.

The private sector is already well-incentivized to pursue most of these strategies. However, this framework highlights two key roles for government: first, to address the critical gaps that industry cannot close alone, and second, to ensure that new regulations do not inadvertently complicate or undermine the industry's own drive for resilience.

Denial

An essential first step in protecting critical infrastructure is ***denial***: ensuring that bad actors do not gain access to the system. Until recently, much of the U.S. government's strategic focus on submarine cable protection has concentrated on this single strategic initiative.

Supply Chain Risks

Specifically, this focus has been on mitigating "supply chain" risks generated by the Chinese Communist Party (CCP), particularly concerning the opto-electric components that form the brains of the cable system.

It is important to distinguish between cable *owners* and *installers*. When media reports state that a company like Google is "building a cable," it means Google has contracted with one of a few specialized firms to manufacture and install the system, which Google will then own and operate. The global market for these installations is highly consolidated, with only four companies accounting for the vast majority of all projects: SubCom (a U.S. company), ASN (France), NEC (Japan), and HMN Tech (China). HMN Tech, formerly known as Huawei Marine, has been the primary target of U.S. government supply chain concerns.

The author of this report lacks the data to determine whether HMN Tech constituted a serious threat to U.S. users of cables. What *is* certain, though, is that the U.S. government's denial strategy has been demonstrably effective. HMN Tech's market share, which was never dominant, has declined over time. This reduction is largely geographic. Due to U.S. government pressure and allied cooperation, HMN Tech has gained little presence outside of its home markets in East Asia and Africa. A comparison of projected builds illustrates this: SubCom is installing or will install cables in almost all parts of the world, while most of HMN Tech's future builds are restricted to shorter, regional systems.

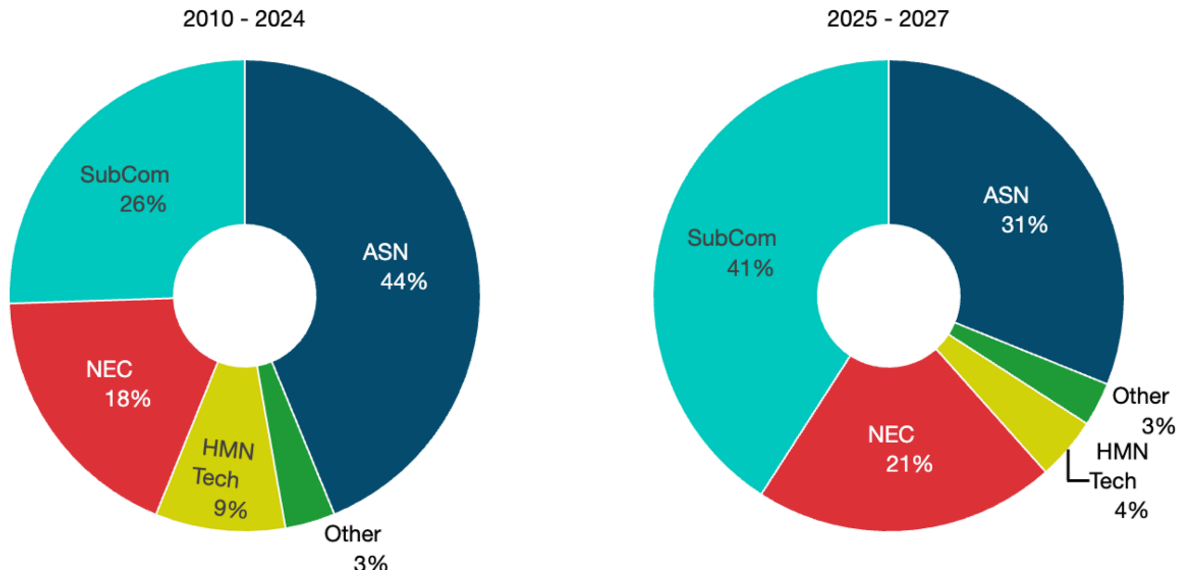
The Limits of a Denial Strategy

There are inherent limits of a denial-only strategy. Much like other critical ecosystems, such as the electric grid or national pipelines, submarine cables cannot be fully hidden. To prevent constant accidental damage from fishing and anchoring, their locations *must* be charted and disseminated to all other seabed users.

Furthermore, while cables in shallow water are armored and buried, they cannot be sufficiently "hardened" to guarantee survivability against all physical threats. A sufficiently heavy anchor dragged with enough force by a large vessel will cause a cable fault, and no amount of steel armoring can prevent it.

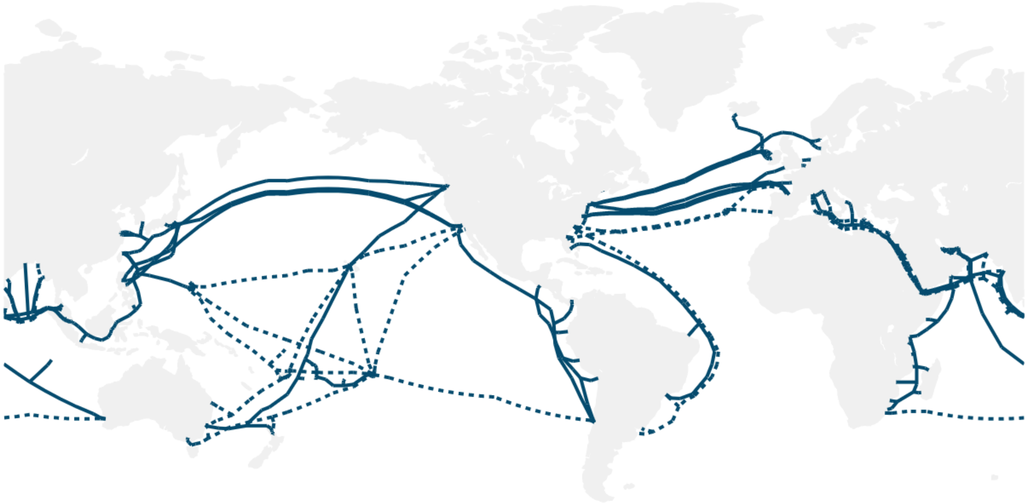
Denial of access is a critical and successful first step in a layered defense. But it does not, and cannot, protect infrastructure from the kinetic, physical-world threats of accidental or deliberate damage. To address those, the strategic arsenal must be widened.

Total Length of Cables by Supplier



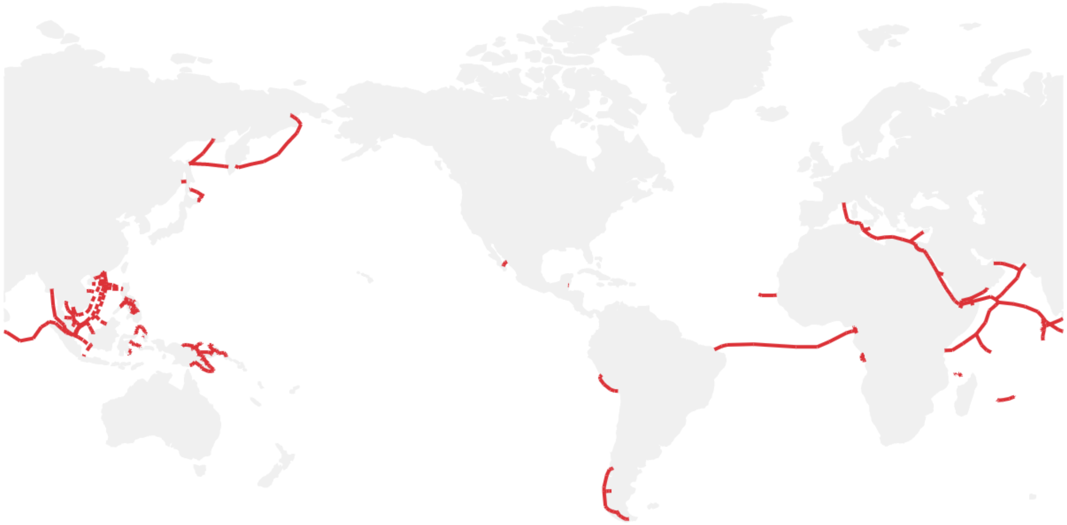
Notes: Data shows aggregate length of new international and domestic submarine cables entering service since 2010, and of planned cables that have been announced.
Source: TeleGeography's Transport Networks Research

Cables Supplied by SubCom



Notes: Cables include existing cables reaching service in 2016-2025 (solid lines) and planned cables (dashed lines).
Source: TeleGeography's Transport Networks Research

Cables Supplied by HMN Tech



Notes: Cables include existing cables reaching service in 2016-2025 (solid lines) and planned cables (dashed lines).
Source: TeleGeography's Transport Networks Research

Diversity

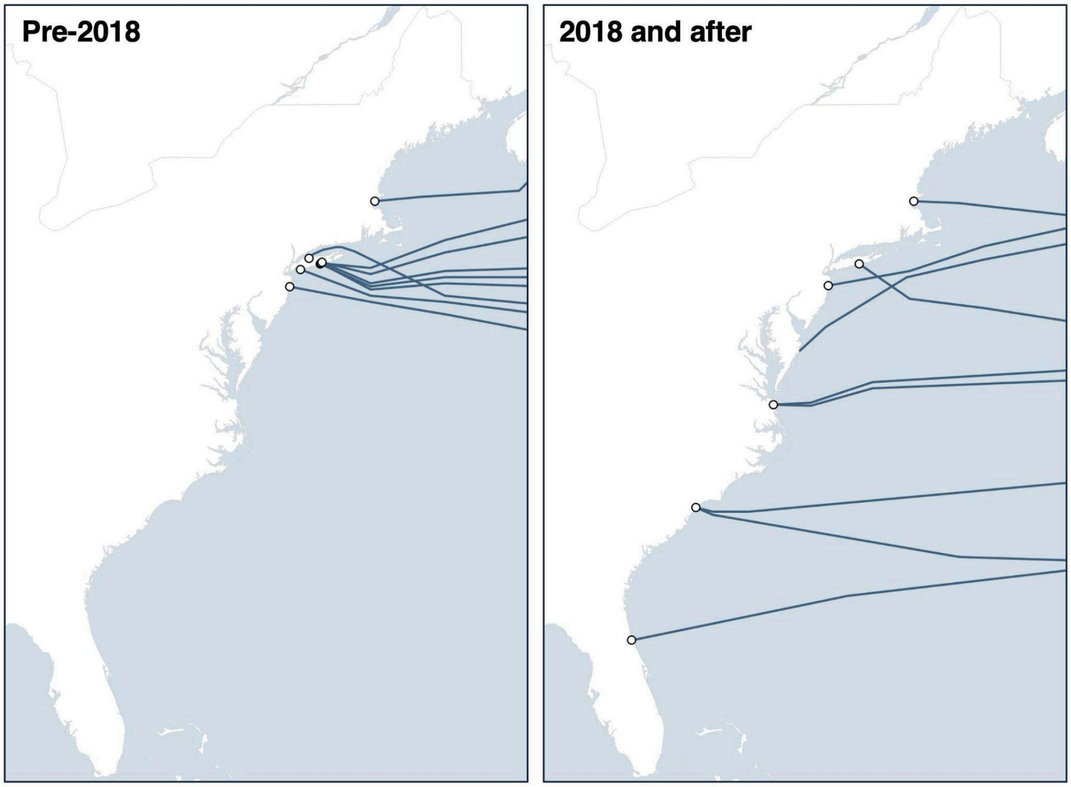
The security and resilience of the U.S. economy and national defense depend on the global network of submarine fiber-optic cables. A key strategic imperative for this resilience is diversity: ensuring that data can be rerouted seamlessly through multiple, geographically separate cable paths in the event of a fault or failure.

In 2000, 30 submarine cables connected to U.S. shores. According to data from TeleGeography, that number now stands at 96, with another 34 cables on their way in the next few years.

Industry-Led Diversification of Cable Landings

True network resilience comes from geographic distribution, not just cable count. A large number of cables provides no meaningful diversity if they all land at the same few choke points, which simply creates a more valuable single point of failure. While the total number of cables has grown steadily over time, the most significant strategic shift has been in the geographic distribution of this infrastructure, driven largely by private-sector investment.

New Landings for Trans-Atlantic Cables



Source: TeleGeography's Transport Networks Research

The fruits of this investment are evident in the Atlantic. Historically, the U.S. East Coast's trans-Atlantic connectivity was highly concentrated in the New York/New Jersey corridor. Today, the landing-point map shows broad distribution, from Canada to the Southeastern U.S., with major new trans-Atlantic systems terminating in states like Virginia (Virginia Beach), South Carolina (Myrtle Beach), and soon, Florida and Maryland.

A Critical Vulnerability: The Risk of Concentration

Despite this progress, significant vulnerabilities remain. The inherent nature of submarine cables means they cannot be entirely hidden, nor can they be armored to guard against all malicious and non-malicious threats. This physical vulnerability is dangerously magnified when critical cables are forced to cluster in "choke points."

A concerning example exists in the waters around the U.K. and Ireland, where many cables are concentrated in a few locations. As one U.K. report notes, a single vessel journeying from Land's End towards Aberystwyth would cross the paths of approximately 20 submarine cables. To mitigate the risks of such high-value, high-concentration targets, governments should review their own policies to determine whether regulations are unintentionally holding back subsea cable providers from connecting to new landing stations, terrestrial routes, and data centers outside these established choke points.

Policy Considerations for a More Resilient Network

The U.S. government has a critical role to play in facilitating this industry-led diversification. However, regulatory and jurisdictional hurdles often hinder these efforts, sometimes even forcing the very clustering that policy should be designed to prevent.

Based on our conversations with industry stakeholders, the following policy considerations would help promote cable diversity:

1. **Reduce Regulatory and Permitting Barriers**. The most significant impediment to building new, diverse cable routes is the complex, lengthy, and often duplicative permitting process. Numerous cable operators have brought up their concern that timescales for installation permits in the U.S. can be unpredictable and excessively long, discouraging investment in new routes. This includes challenges with inter-agency processes, such as the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (commonly known as "Team Telecom").

   Congress is beginning to act on these problems. S.2873, the "Undersea Cable Protection Act of 2025," and its House counterpart, H.R.261, are first steps. These bills would eliminate duplicative permitting for cable installation and repair in federally protected waters managed by the National Oceanic and Atmospheric Administration (NOAA).

2. **Establish Clear Federal Jurisdiction**. A primary source of regulatory delay is jurisdictional confusion. As highlighted by the International Cable Protection Committee (ICPC), industry operators are often faced with a confusing array of federal, state, and local agencies. In the U.S.,

the Federal Communications Commission serves as an *initial* point of contact for prospective cable operators seeking to build new subsea networks, but there is no single entity truly empowered to shepherd cable operators through a bewildering tangle of rules.

The cable industry has long wished for a single point of contact for submarine cables within the federal government. This lead agency should not merely be for permitting, but for all issues related to installation, repair, and protection. This lack of a central authority is a known problem in other countries as well; a U.K. report on cable security recently cited "palpable uncertainty" about "jurisdiction and primacy between departments," a challenge that is mirrored in the U.S.

3. **Promote and Assist with Marine Spatial Planning**. Submarine cables must share the seabed with numerous other users, including commercial fishing, renewable energy, and potential future deep-seabed mining. This creates a complex environment where cable routes are often limited.

   The U.S. government should formally identify submarine cable operators as critical stakeholders in all marine spatial planning and policymaking. Rather than allowing government regulation (such as the designation of Marine Protected Areas) to inadvertently force cables into predictable, high-risk corridors, policy should be used to proactively optimize routes for geographic diversity. By assisting industry with spatial planning, the government can help de-risk new routes and build a network that is inherently more resilient to both accidental damage and malicious attack.

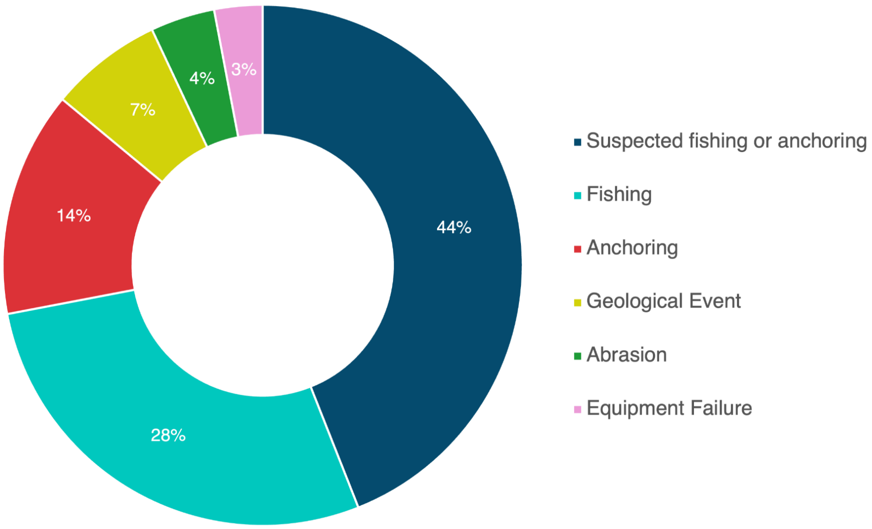
Deterrence

To supplement efforts in building network diversity, a parallel strategy of ***deterrence*** is required to prevent cable damage from both hostile and accidental acts.

Primary Causes of Accidental Damage

It is critical to understand that the vast majority of cable damage is accidental, not malicious. The seafloor is a dangerous environment for undersea fiber-optic cables; the network experiences roughly 200 faults each year, or an average of four per week.

Cause of Submarine Cable Faults



Source: ICPC Global Cable Repair Data Analysis 2025

These incidents are overwhelmingly concentrated in or near coastal waters. According to the International Cable Protection Committee (ICPC), 43% of all cable faults occur within a nation's 12-nautical-mile territorial waters, and 98% occur within its 200-nautical-mile Exclusive Economic Zone (EEZ). This is where cables intersect with the highest volume of human maritime activity.

- **Commercial Fishing**: This is a leading cause of damage. The risk comes not from nets, but from the heavy gear used in bottom-contact fishing. This includes bottom trawling, where heavy trawl doors are dragged to keep nets open and can plow through the seabed, snagging cables. Dredging for shellfish uses heavy metal rakes designed to dig into the seafloor, which are highly effective at hooking cables. Other risks include the massive anchors used to secure stow nets and the grapnels fishermen use to recover lost gear, both of which can snag and break cables.

- **Anchor Dragging**: While some observers have expressed skepticism that a crew could be so negligent as to allow an anchor to drag for long distances, industry records show this is a well-documented and frequent type of accident (see the table below).

  This risk is amplified by the age and condition of vessels. Poor vessel condition is a particularly acute problem in the Baltic Sea, where shallow waters leave cables vulnerable to anchor drag. According to an Atlantic Council report, the rise of the "shadow fleet" servicing Russia has seen the average age of crude oil tankers departing from Kaliningrad increase from 15.4 years in 2020 to 29.3 years in January 2024. These older, poorly maintained, and poorly crewed vessels pose a significant and growing risk.

Selected Accidents Involving Anchor Drag Damage to Undersea Infrastructure

Date	Location	Vessel	Accident Details & Cause	Infrastructure Damaged
2002	U.S. East Coast (Philadelphia to NYC)	Aconcagua	Anchor dragged in a gale. Cause: Improper stowage (only brake was set, no chain stopper).	3 telecom cables (linking US-Europe)
June 2007	North East Coast, U.K.	Young Lady	While weighing anchor in bad weather, the windlass hydraulic motor exploded. Cause: Equipment failure.	1 gas pipeline (snagged as anchor ran out)
2008	Off Sicily, Italy	Unnamed (large oil tanker)	Vessel dragged its anchor for 300 km in water depths down to 180m.	6 telecom cables
2008	North Channel, Irish Sea (UK)	MV Mornes	Vessel dragged its anchor for at least 50 km.	2 telecom cables (also crossed 2 power cables and 1 pipeline)
2012	Red Sea	Blue Princess	AIS showed the vessel dragging its anchor over a 12-hour period, with its speed dropping to zero as it snagged cables.	3 telecom cables (SEA-ME-WE 3, EASSy, EIG)
Mar 2016	Isles of Scilly, U.K.	Unnamed	Vessel dragged its anchor.	Telecom and power cables (cutting electricity to the islands)
Mar 2017	Land's End, U.K.	Romy Trader	Vessel dragged its anchor while underway for at least 25 km.	4 telecom cables and 1 power cable
Apr 2018	Lake Michigan, U.S.	Clyde S. VanEnkevort	Dragged anchor for 36 hours over 600 km. Cause: Human error (crew failed to secure 2 of 3 anchor mechanisms).	3 power cables and 2 oil pipelines
Jan 2025	Baltic Sea (off Gotland, Sweden)	Vezhen	Bulk carrier dragged anchor after last of 3 safety devices failed in bad weather. Cause: Equipment failure (2 devices were already broken) & weather. Crew was unaware as autopilot compensated.	1 telecom cable (Sweden-Latvia)

Sources: International Cable Protection Committee (https://iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/), European Submarine Cable Association (https://www.linkedin.com/pulse/anchors-damaging-cablesis-drag-europeansubseacablesassociation-avwue), news reports on Swedish prosecutor findings

- **Illegal Sand Dredging**: Illegal dredging to obtain seabed sand presented a major threat to cables around the Matsu Islands of Taiwan in the early 2020s. Sand is the world's second most extracted resource, a critical component for land reclamation, glass, and cement. The scale of this demand is staggering; as detailed in *Foreign Policy* journal, China consumed more cement in just three years than the United States used during the entire 20th century.

However, this risk has been proven to be highly responsive to deterrence. Following a 2021 law change in Taiwan that increased penalties for illegal mining to a maximum of seven years in jail and a $3.2 million fine, the *Taipei Times* documented a dramatic decline in incidents: from a peak of 3,991 vessels in 2020 down to just 224 in 2022.

Similarly, cable faults from anchor drags have seen a sharp decrease in 2025 after NATO allies (in particular, Sweden, Finland, and Estonia) stepped up investigation and enforcement of cable protection.

Policy Considerations

To address these threats, industry bodies have proposed a number of policy considerations for governments.

1. **Prohibit High-Risk Activities Near Cables**: A primary consideration is to prohibit high-risk fishing activities—such as the deployment of heavy fishing equipment and vessel anchors—in the immediate proximity of charted submarine cables.

2. **Avoid Mandatory Protection Zones**: Conversely, the ICPC reports that operators generally disfavor mandatory cable protection zones or corridors. The concern is that these zones provide insufficient spatial separation for installation and maintenance and, paradoxically, encourage the geographic clustering of cables, which magnifies the risk of a single incident damaging multiple systems.

3. **Establish Legal Accountability and Penalties**. The 1884 Convention on the Protection of Submarine Telegraph Cables requires state parties to establish offenses for cable damage. However, the United States has not updated its penalty amounts for more than 130 years. The current penalties—a maximum of $5,000 for intentional damage or $500 for negligent damage—are woefully, almost comically, insufficient as a deterrent.

   Congress has begun to recognize this shortcoming. H.R.3479, the “Safeguarding Essential Cables through Undersea Risk Elimination (SECURE) American Telecommunications Act,” would significantly increase these outdated penalties for both willful and negligent damage, creating a credible deterrent.

Detection

A comprehensive security strategy for submarine cables also relies on ***detection***: the ability to use monitoring systems to identify and locate cable faults or threats.

An effective detection strategy serves a dual purpose: proactively preventing damage before it occurs and, failing that, conducting forensic analysis to identify the responsible party. Real-time monitoring can be used to warn vessels away from critical infrastructure, while post-event analysis provides the necessary data to hold a vessel accountable.

New Technologies

Traditionally, monitoring has relied on the Automatic Identification System (AIS), a shipboard transponder that broadcasts a vessel's identity and location. The primary weakness of AIS, however, is that it is an active system that can be, and often is, disabled by uncooperative or malicious actors.

To supplement AIS, the industry is developing advanced fiber-optic sensing technologies. These systems allow the fiber-optic cable *itself* to be used as a vast, real-time sensor. This technology detects minute changes in light signals to "listen" for acoustic signatures, such as the sound of a ship's propeller, the drop of an anchor, or the longer-term environmental threat of a cable chafing against a rock.

This technology also offers a profound public-good benefit: scientific monitoring and disaster early warning. The same fiber-optic sensing equipment has proven highly effective both at sensing seismic activity and at providing advanced detection of tsunamis.

Policy Considerations

1. **Provide regulatory certainty.** The capabilities of these new detection technologies have expanded rapidly, and industry has not yet coalesced around a unified stance on their deployment. While some operators are early adopters, many remain concerned that widespread use of advanced monitoring systems could complicate their permitting process. A primary worry is that this equipment may prove *too* effective, gathering sensitive data on vessel movements that could create new regulatory or data-handling burdens.

   Therefore, the most important action the government can take is to provide regulatory certainty. Industry reports suggest a need for the government to work with operators to determine what detection capabilities would be allowed under standard cable permitting. This collaborative approach could speed adoption of these valuable detection technologies.

2. **Continue to enforce responsible AIS use**. To supplement other sources of maritime awareness data, the industry recommends that governments require the continuous use of AIS. This policy might include establishing clear criminal and civil penalties for any operator who intentionally disables these systems. This policy consideration aligns with the existing legal framework, as U.S. law already mandates AIS use for many commercial vessels.

Deployment

Even with a multi-pronged strategy to build diversity, deter threats, and detect actors, it is inevitable that cables will continue to suffer damage. This requires a final strategic imperative: maintaining the capability to *deploy* resources and repair critical infrastructure rapidly.

A Robust and Improving System

Industry reports indicate that the capability and reliability of the global cable network are strong and improving.

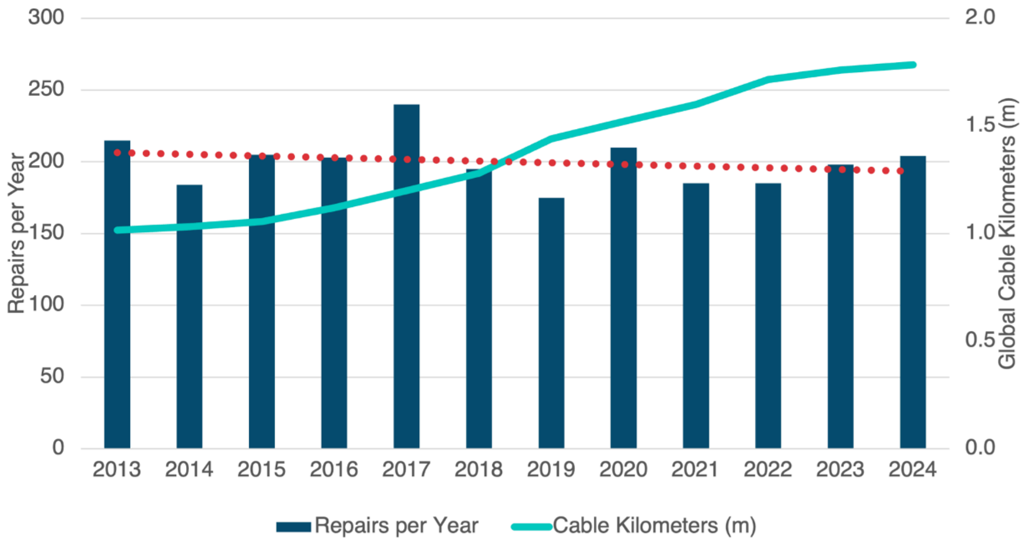
- **A Ready Fleet:** The submarine cable industry has developed and maintains a specialized fleet of 62 installation and repair vessels. A recent report from Infra-Analytics and TeleGeography, “The Future of Submarine Cable Maintenance,” identified the need for future investment to replace aging ships and improve service in regions prone to repair queuing during simultaneous faults. Additional investment is needed to train skilled technicians and cable ship crew.

  Despite these long-term fleet modernization challenges, the industry’s underlying process for cable repair is proven, well-practiced, and effective. A 2025 U.K. parliamentary report (HC 723 / HL Paper 179) affirmed this capability, finding the standard industry response to be “efficient, well tested and robust.”

- **Decreasing Faults:** Despite recent media hype about cable faults, the total number of annual repairs has slightly *decreased* over the last decade. This decline is particularly noteworthy given that the total kilometers of cable in service have increased by over 50% during the same period, indicating a sharp decrease in the number of faults per kilometer.

- **Increased Reliability:** Cable reliability has significantly improved, thanks in large part to the industry-led move toward deeper and more extensive burial in high-risk shallow seas. While this has come at considerable expense—cable burial (only 12% of total global cable length) accounts for an estimated 60% of overall marine installation time and cost—the investment has yielded clear results.

Global Repairs per Year



Source: ICPC Global Cable Repair Data Analysis 2025

Growing Bureaucratic Delays

Some troubling trends lurk behind improvements to repair. While the *rate* of faults has fallen, the *time* it takes to conduct a repair has noticeably increased.

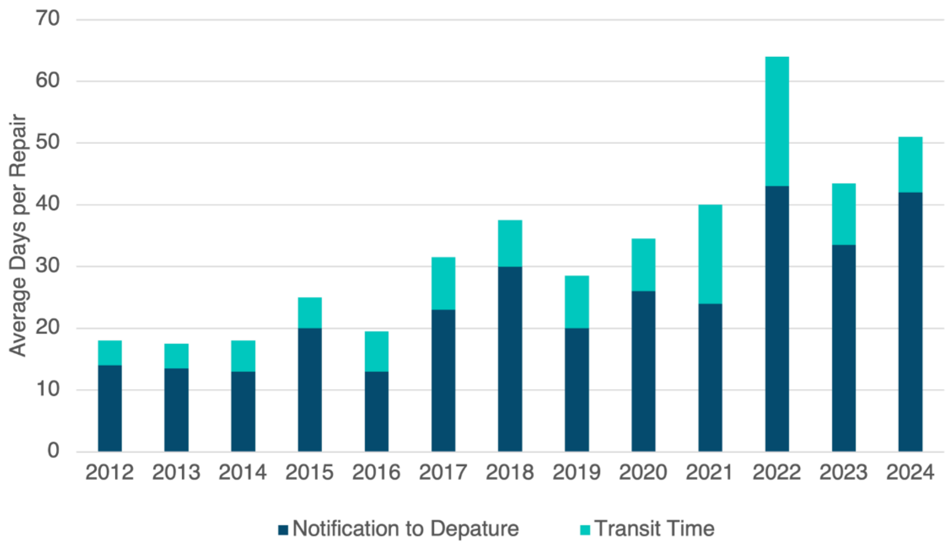
According to industry data, the average global delay from the time a fault occurs to the time a repair vessel begins work is approximately *one and a half months*. The fact that Americans rarely experience service downtime, even with such inefficiency, is a testament to the high degree of network diversity connecting the country. However, given the criticality of this infrastructure, such a long delay represents a dangerous vulnerability.

This delay is not due to a lack of ships or slow transit. Data in the chart below shows that “Transit Time”—the time it takes a vessel to steam to the fault—accounts for only a small percentage of the wait. The primary culprit is the “Notification to Departure” time, a delay often attributable to permitting delay.

This problem is most acute in regions with onerous regulations. Common causes for delay include cabotage rules (Laws that restrict maritime activities to domestically-flagged vessels), complex operational permitting, and port duties and clearances.

The U.S. is generally regarded as having an industry-friendly environment for repairs, with delays less severe than the global average. The global increase in repair time is largely driven by a growing number of faults occurring in Asia and the Middle East, where such regulations can be burdensome.

Average Time before Repair



Source: ICPC Global Cable Repair Data Analysis 2025

Policy Considerations

Because U.S. connectivity relies on the health of the *entire* cable, including its landing point in a foreign country, it is in the U.S. national interest to address both domestic and foreign delays.

1. **Harmonize Federal Permitting for Cable Repairs:** Operators currently face a fractured and duplicative system, where an emergency repair in one jurisdiction is a simple notification, while in another—particularly in federally protected waters—it can be forced into a complex, months-long review. This inconsistency creates uncertainty and can stall the restoration of critical infrastructure. Congress can resolve this conflict by ensuring a unified, fast-track emergency authorization for repairs.

2. **Avoid New Mandates that Increase Repair Times:** The U.S. must avoid imposing new regulations that would critically damage its own repair capacity. For example, attempts to impose U.S. flag requirements for cable ships would result in massive delays and expense, as a sufficient fleet of these highly specialized, U.S.-flagged vessels does not exist.

3. **Work with Foreign Partners to Speed Global Repairs:** A major source of delay affecting cables carrying U.S. traffic occurs in the territorial waters of foreign partners. The U.S. government should focus diplomatic efforts to urge nations to exempt specialized cable vessels from the most time-consuming regulations: domestic cabotage (cargo) laws, crewing restrictions, and customs duties.

Government/Industry Cooperation

The Success of Industry-Led Resilience

A central finding of this analysis is that the private sector's incentives are already deeply aligned with the government's national security goals. The companies that have built the world's internet have done so not primarily from a sense of patriotism, but from a powerful and effective sense of "enlightened self-interest." This is a significant strategic advantage, as it means the private sector incentive to build and maintain network resilience already exists without the need for burdensome government mandates.

This alignment is straightforward: downtime is financially catastrophic for cable owners. For content providers like Google and Meta, submarine cables are the global backbones supporting the paid services and advertisements that generate the bulk of their revenue. For traditional carriers, any downtime can trigger severe financial penalties in their contracts with customers. With cable repairs costing as much as $1 million per day, the business case for resilience is absolute.

This financial incentive has translated into a robust, multi-billion dollar private investment in network resilience. This includes not just building new, diverse cables, but hardening landing stations, pioneering strong self-governing mechanisms for cable safety, cooperating with other seabed users, innovating with new detection systems, and developing well-proven repair mechanisms.

A Strategic Asset Under Waning Control

This industry-led system has cemented America's central position in global communications, which is a tangible strategic asset. This centrality is a form of economic hard power, ensuring the U.S. remains the primary hub for the global data economy.

However, this central position is not guaranteed and, by some metrics, is already waning. According to research from TeleGeography, while nearly 80% of the world's intercontinental communication flows still traverse or terminate in the United States, that figure is down from 97% in 2005. Similarly, the U.S. share of all cross-border data flows has fallen from 43% to 25% in the same period.

The U.S. is fortunate that industry coalesced around our country as the world's global switching hub, a development fostered by early government investment in networking technology and a historically business-friendly regulatory climate. But there is no structural imperative that prevents the industry from migrating away. Placing burdensome regulations on cable investors—even if well-intentioned and designed to *strengthen* security—could inadvertently chase them to other, more accommodating nations. This would undermine the very resilience that industry has spent billions to build across the dozens of cables that now connect to the U.S.

The Imperative for a Government-Industry Partnership

Effective regulation requires a partnership with industry, yet the U.S. is falling behind in facilitating infrastructure growth. Data shows that federal permitting timescales have more than doubled in five years, with U.S. processes now moving even more slowly than national regulators in Egypt, India, and Indonesia. These delays, often measured in *years*, are partially attributable to the “Team Telecom” process. This overlapping, multi-agency process focuses intensely on a strategy of “Denial” regarding foreign ownership and supply-chain risks. However, a security strategy that relies solely on Denial is incomplete. When regulatory hurdles prevent the timely construction of new, diverse routes, the government undermines the broader strategic goal of a resilient, redundant network.

Industry has been the leader in cable security and has built a resilient global system; it looks to the government as a reliable support partner. This relationship need not be confrontational. If the United States is to maintain its strategic centrality and ensure the resilience of its most critical network infrastructure, it cannot be.

Acknowledgements

The analysis in this document is informed by dozens of interviews with industry professionals conducted over the past several years. While the undersea cable community holds a diversity of views on the policy prescriptions that would best serve cable security, the author has taken care to fairly represent the *general* consensus. Any errors or misinterpretations are his own.

The author extends particular gratitude to the leadership of the International Cable Protection Committee (ICPC) and the European Submarine Cable Association (ESCA) for their assistance. The ICPC "Best Practices for Governments" document is the single-best blueprint for improved public/private cooperation. Many of the recommendations in the "Best Practices" document were endorsed in the 2024 "New York Principles on Undersea Cable Security and Resilience," a set of non-binding guidelines co-sponsored by the United States and affirmed by over thirty other countries.

Finally, the author would also like to thank Lieutenant Noah Gratias for the valuable insights gleaned from his forthcoming research contrasting submarine cable faults in the Taiwan Strait with typical CCP gray zone operations.

About TeleGeography

TeleGeography is a telecommunications data provider known for independent analysis. The company's mission is to advance the communications landscape by delivering trusted data to its customers.

TeleGeography also makes significant resources freely available to the public. These include the "Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies" eBook and the widely-used, interactive Submarine Cable Map, which is updated frequently.