TeleGeography

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.

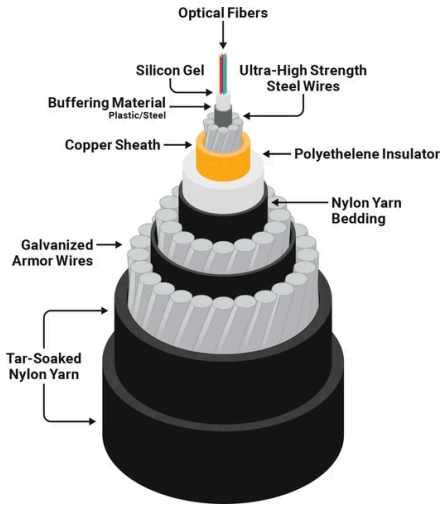
How Cables Work

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.

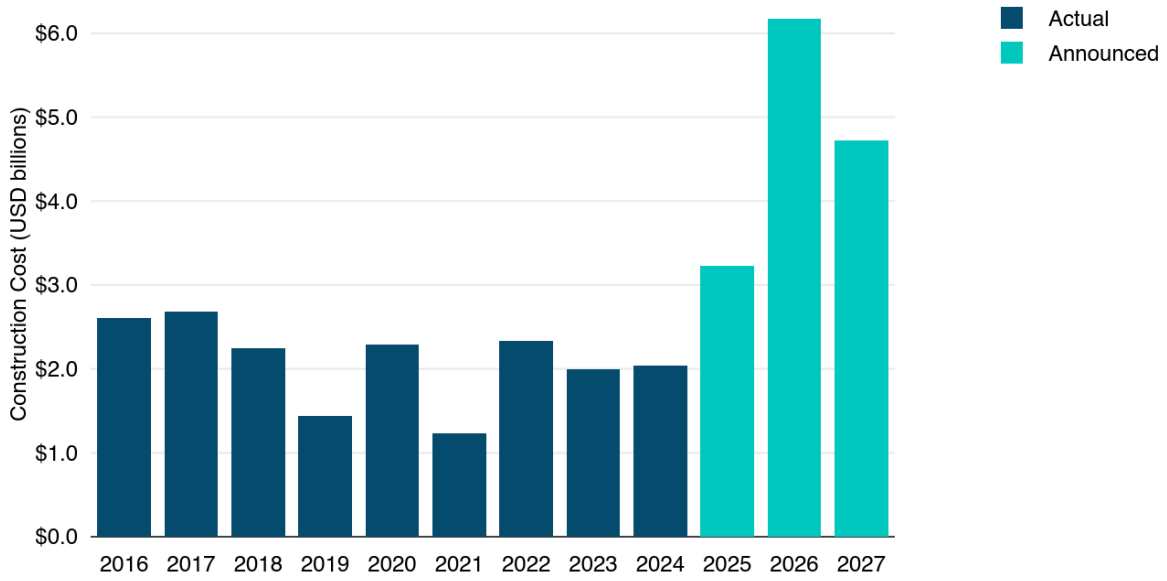
The United States currently has 96 active cables landing on its shores. What's even more telling is the future pipeline: the 34 new cables planned for the U.S. represent nearly a third of all publicly announced projects worldwide, underscoring America's critical importance as a global data hub.

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.

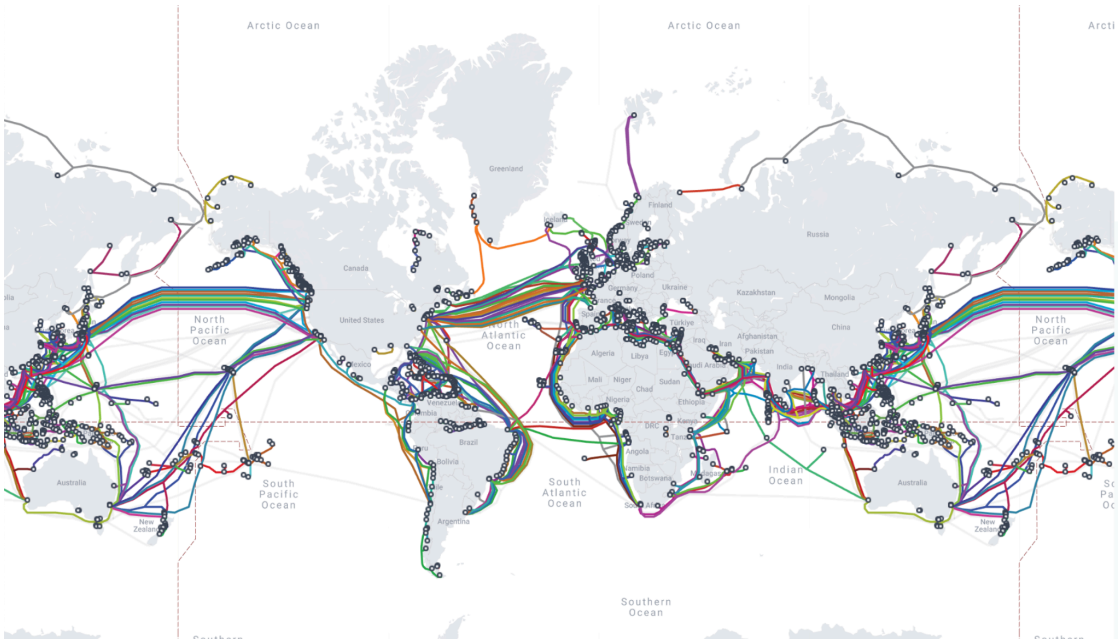
The charts and maps below illustrate the pattern of cable investments.

Combined Construction Costs of Cables Entering Service



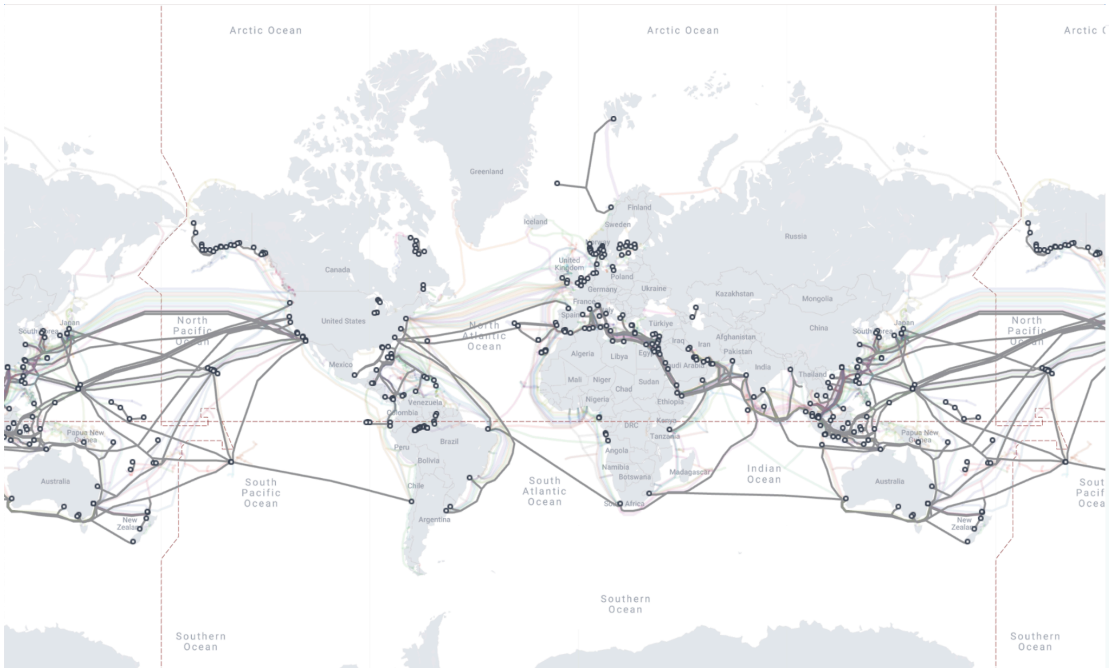
Notes: Total construction costs of all international and domestic submarine cables entering service in designated years. Construction costs exclude the cost of subsequent capacity upgrades and annual operational costs. 2025-2027 construction costs based on announced contract values and TeleGeography 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.

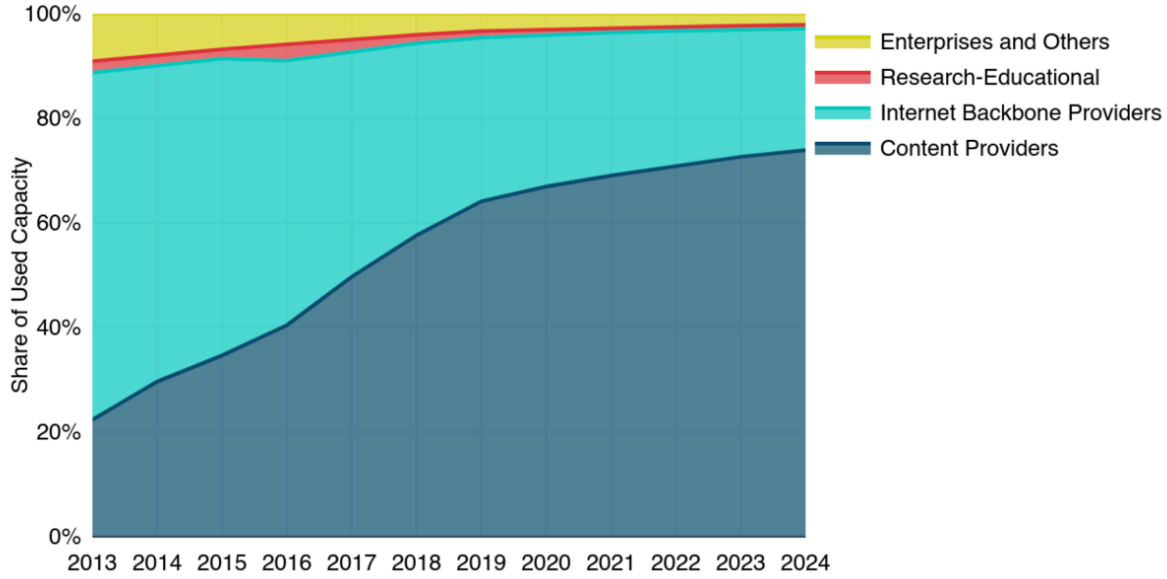
Cables were traditionally owned by telecom carriers who would form a consortium of all parties interested in using the cable. In the late 1990s, an influx of entrepreneurial companies built many private cables and sold off the capacity to users.

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.

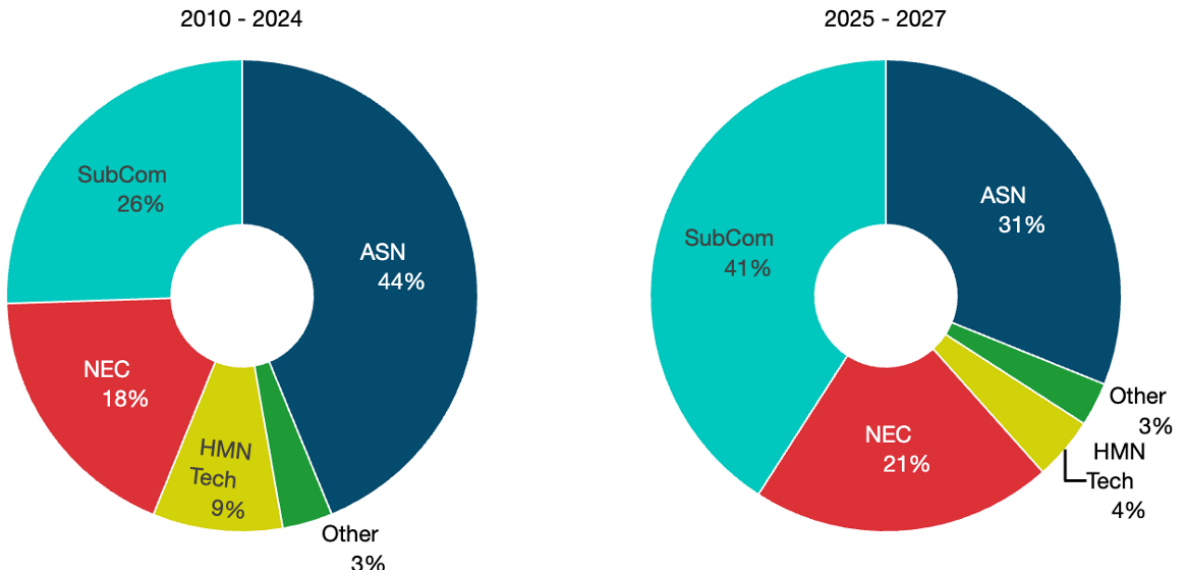
The Limits of a Denial Strategy

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.

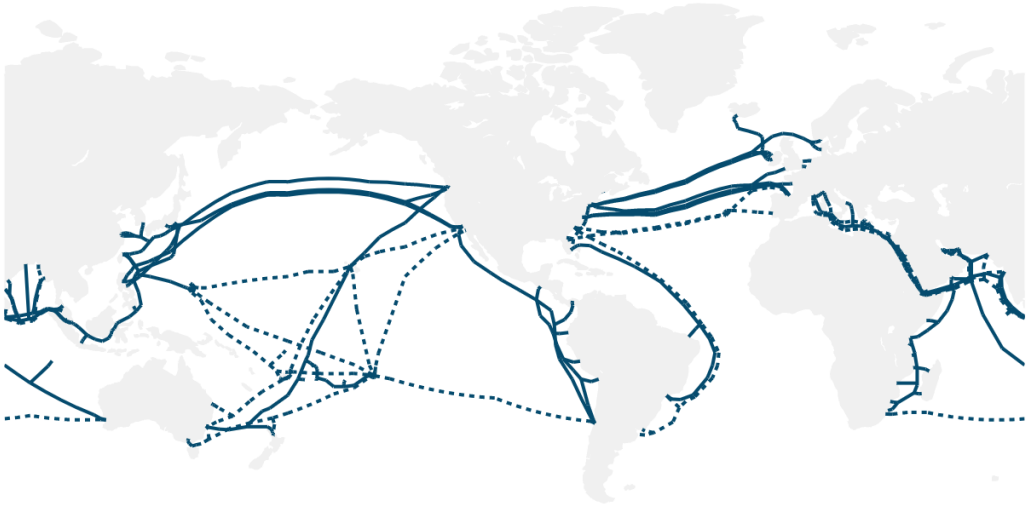
Denial of access is a critical and successful first step in a layered defense. But it does not, and cannot, protect infrastructure from the kinetic, physical-world threats of accidental or deliberate damage. To address those, the strategic arsenal must be widened.

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

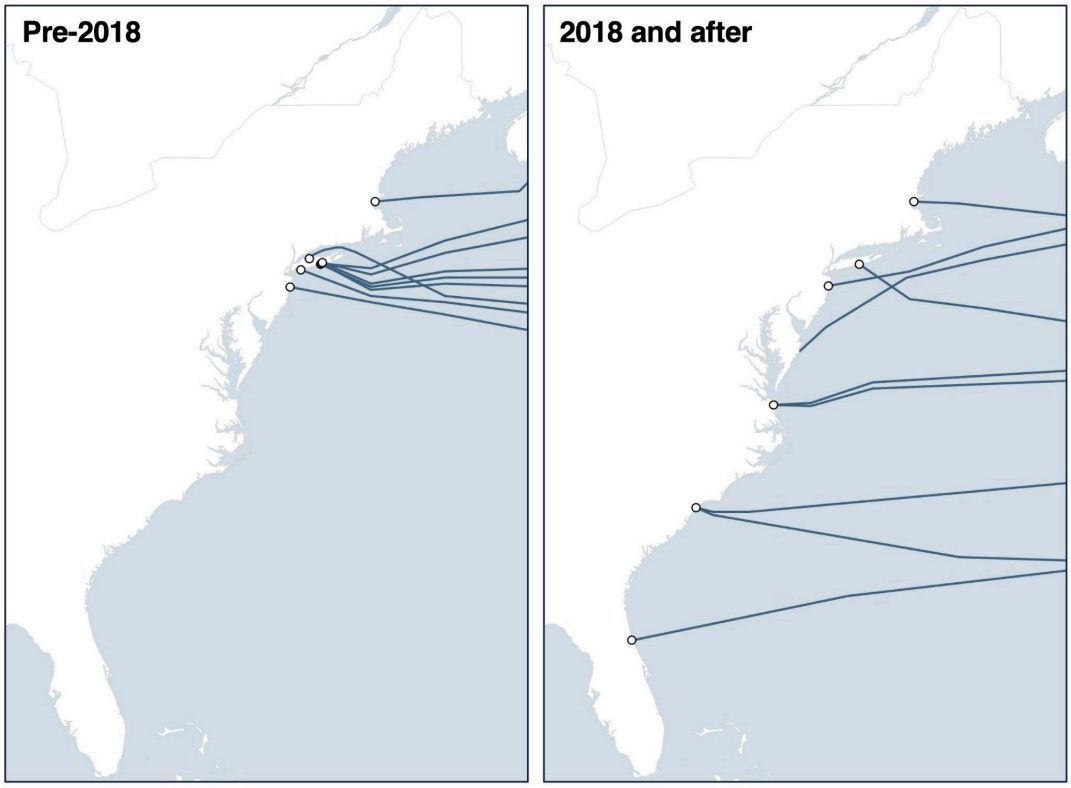
The security and resilience of the U.S. economy and national defense depend on the global network of submarine fiber-optic cables. A key strategic imperative for this resilience is diversity: ensuring that data can be rerouted seamlessly through multiple, geographically separate cable paths in the event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

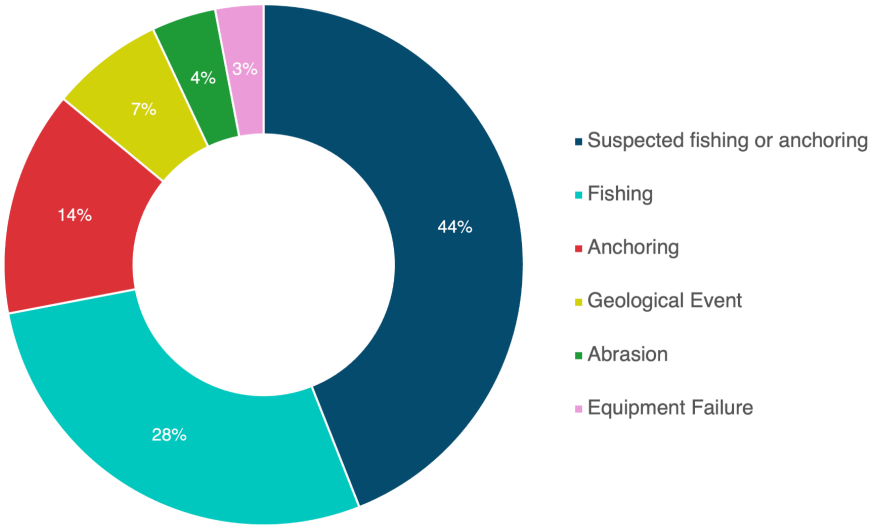
Deterrence

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.

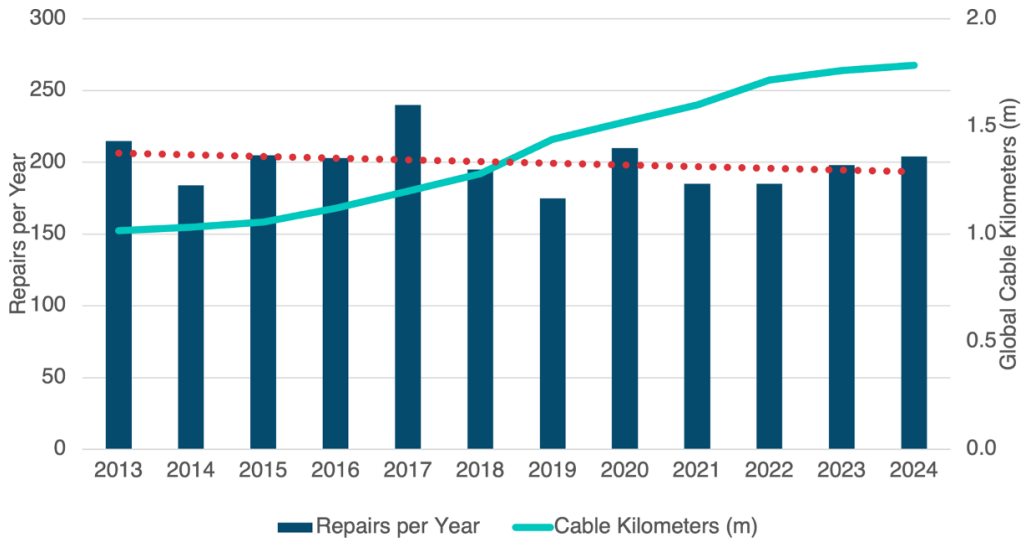
- **A Ready Fleet:** The submarine cable industry has developed and maintains a specialized fleet of 62 installation and repair vessels. A recent report from Infra-Analytics and TeleGeography, "The Future of Submarine Cable Maintenance," identified the need for future investment to replace aging ships 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.

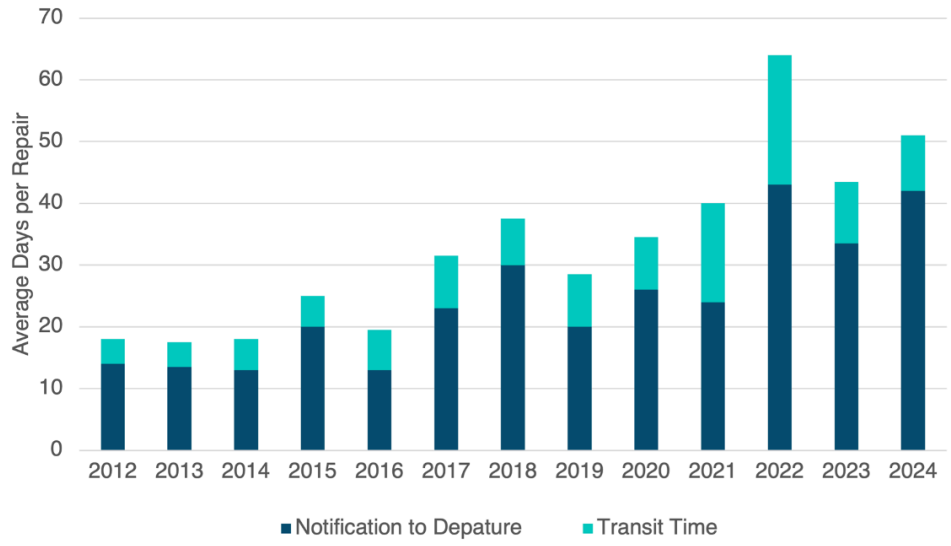
According to industry data, the average global delay from the time a fault occurs to the time a repair vessel begins work is approximately *one and a half months*. The fact that Americans rarely experience service downtime, even with such inefficiency, is a testament to the high degree of network diversity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

TESTIMONY BEFORE THE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY AND
CYBERSECURITY AND INFRASTRUCTURE PROTECTION

An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure

November 20, 2025

Statement by Matthew Kroenig

Vice President and Senior Director, Scowcroft Center for Strategy and Security, Atlantic Council
Professor of Government and Foreign Service, Georgetown University

Chairman Gimenez, Chairman Ogles, Ranking Member McIver, Ranking Member Swalwell, distinguished members of the committee, thank you for the opportunity to testify on the important topic of foreign adversary threats to subsea cable infrastructure.

I want to assist your work by sharing insights gleaned from my more than two decades of experience working on US national security policy at the Central Intelligence Agency, the Department of Defense, the Congressional Commission on the Strategic Posture of the United States, and now as a professor at Georgetown University, and vice president and senior director of the Atlantic Council's Scowcroft Center for Strategy and Security.

I lead a center responsible for global strategy and security, so I will focus my remarks on the geopolitical and national security dimensions of this challenge.

My message today is simple: China's and Russia's threats to subsea cables present a serious challenge to the global communications and energy systems that underpin US and allied security, prosperity, and way of life. The United States needs a more effective strategy to deter and defeat adversary threats to subsea cables.

Since World War II, the United States and its allies have built and defended an international system that has delivered unprecedented peace, prosperity, and freedom to the American people. The design of global undersea cable infrastructure was established in a more peaceful time in which it was assumed that major powers had a shared interest in cooperation and would behave responsibly.

Unfortunately, the global security environment has greatly deteriorated in recent years. The People's Republic of China may pose the greatest threat the United States has ever faced. It is a comprehensive challenge that includes economic, technological, ideological, diplomatic, and military dimensions. Moreover, China is working in coordination with an Axis of Aggressors, Russia, Iran, North Korea, and Venezuela.

China seeks to dominate the digital infrastructure of the 21st century, including in subsea cables, to provide it with economic, espionage, military, and geopolitical advantages.

China and Russia wage gray zone warfare to coerce vulnerable US allies and partners and to induce caution in Washington about intervening on their behalf. Tactics in this war include Russia's likely involvement with the bombing of a rail line in Poland earlier this week, China's almost daily military incursions into Taiwan's territorial waters and airspace, and, increasingly, the cutting of subsea cables.

Russian-linked vessels have cut many undersea cables in the Baltic Sea in recent years. On Christmas Day last year, for example, an oil tanker crossed the Gulf of Finland, damaging four cables. In 2023, PRC-registered ships severed two undersea cables, forcing Taiwan's Matsu Islands offline. The Islands 14,000 residents spent weeks with limited connectivity. Sending a simple text message took hours.

The United States is not immune. As tensions escalate with Venezuela, for example, a Maduro-linked vessel could drag an anchor off the US coast, cutting cables in shallow water. There is nothing technologically difficult about this scenario.

Moreover, as tensions escalate, there is a risk of major conflict with China, or Russia, or both simultaneously. In the event of war, China and Russia could undertake a more systematic campaign to sever cables to the United States and its allies.

Roughly 95% of global internet traffic relies on undersea cables. Attacks on these cables disrupt connectivity and with it the functioning of modern society, including: communications, financial and business transactions, energy supplies, global supply chains, military operations, and daily life in general.

Currently, the US and its allies lack a coordinated and effective strategy to deal with this threat. As a starting point, Congress could task the executive branch with developing a strategy to secure subsea cables. It could also designate the Department of Homeland Security as a single hub to coordinate and manage undersea cable protection.

Such a strategy could include three key pillars:

The first pillar is resilience. The United States and its allies need to develop a more resilient subsea cable infrastructure. This could include de-risking from Chinese-owned or maintained cables and cables that route to mainland China. This could include building redundancy by laying additional cables and by establishing backup sources of connectivity, such as satellite and microwave links. This could also include an enhanced repair capacity to bring damaged cables back online more quickly.

A more effective approach to resilience can not only limit the negative impact from severed cables, but also contribute to deterrence by signaling to adversaries that we can bounce back from any attack.

A second pillar is monitoring. The United States and its allies need to maintain presence near vulnerable cables to monitor, attribute, interdict, and deter potential attacks. If adversaries understand that attacks are likely to be interdicted or attributed, they are less likely to make the attempt in the first place. NATO's new Baltic Sentry mission and Taiwan's stepped-up coast guard patrols show the value of increased presence. Finnish authorities took physical control of the above-mentioned oil tanker last December, preventing additional damage. The US Coast Guard could likewise step up patrols and exercises near vulnerable subsea cables, especially off the coasts of New York, New Jersey, Florida, and Southern California. These patrols can be multidomain and enhanced with new technology, such as unmanned systems and AI platforms, to help monitor threats to subsea cables.

The third pillar is accountability. If foreign commandos were to sabotage infrastructure on the US homeland, Washington would not limit its response to repairing the damage. It would hold the perpetrators accountable. The same logic applies to attacks on subsea cables. The United States and its allies must find creative ways to impose costs on states that attack subsea cables as a tool of statecraft and those who help them carry out attacks. Effective deterrence requires that perpetrators understand that their actions carry consequences.

Appended to this statement is a copy of *Cyber defense across the ocean floor: The geopolitics of submarine cable security*, an Atlantic Council report that explores these issues in greater detail and provides actionable recommendations.

I am honored that the Committee on Homeland Security has invited me to share my views on these challenges, and I look forward to taking your questions.

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

CYBER DEFENSE ACROSS THE OCEAN FLOOR

The Geopolitics of Submarine Cable Security

Justin Sherman

Scowcroft Center for Strategy and Security

*The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.*

Cyber Statecraft Initiative

*The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.*

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

CYBER DEFENSE ACROSS THE OCEAN FLOOR

The Geopolitics of Submarine Cable Security

Justin Sherman

ISBN-13: 978-1-61977-191-8

Cover: Shutterstock/Vinko93

September 2021

Table of Contents

Executive Summary

The vast majority of intercontinental global Internet traffic—upwards of 95 percent—travels over undersea cables that run across the ocean floor. These hundreds of cables, owned by combinations of private and state-owned entities, support everything from consumer shopping to government document sharing to scientific research on the Internet. The security and resilience of undersea cables and the data and services that move across them are an often understudied and underappreciated element of modern Internet geopolitics. The construction of new submarine cables is a key part of the constantly changing physical topology of the Internet worldwide.

Three trends are increasing the risks to undersea cables' security and resilience: First, authoritarian governments, especially in Beijing, are reshaping the Internet's physical layout through companies that control Internet infrastructure, to route data more favorably, gain better control of internet chokepoints, and potentially gain espionage advantage. Second, more companies that manage undersea cables are using network management systems to centralize control over components (such as reconfigurable optical add/drop multiplexers (ROADMs) and robotic patch bays in remote network operations centers), which introduces new levels of operational security risk. Third, the explosive growth of cloud computing has increased the volume and sensitivity of data crossing these cables.

The US government, therefore, has a new opportunity and responsibility—in coordination with the US private sector and with allies and partners abroad—to significantly increase its involvement in protecting the security and resilience of undersea cables. As the White House increasingly focuses on cybersecurity threats to the nation and the global community, including from the Chinese and Russian governments, it must prioritize investing in the security and resilience of the physical infrastructure that underpins Internet communication worldwide. Failing to do so will only leave these systems more vulnerable to espionage and to potential disruption that cuts off data flows and harms economic and national security. This report makes this argument drawing on policy and technological research, interviews with key stakeholders, and empirical data collected and subsequently analyzed on the 475 undersea cables deployed around the world (at the time of writing).

It offers eight concrete recommendations for the US government, working with the US private sector and allies and partners worldwide, to better protect the security and resilience of the world's undersea cables: Congress should give more authorities and funding to the committee screening foreign cable owners for security risks, and should consider more funding for the Cable Ship Security Program; the executive branch should promote baseline security standards for remote cable management systems; the Federal Communications Commission should invest more resources in interagency cooperation on resilience threats to cables; the State Department should pursue confidence-building measures for cables and conduct a study on building cables into more capacity-building work; US-based cable owners should create an information sharing analysis center to share threat information; and Amazon, Facebook, Google, and Microsoft should create and publish strategies on better protecting cables' security and resilience.

As the Internet comes under unprecedented authoritarian assault, and societal dependence on the web grows in the absence of robust and ecosystem-wide cybersecurity, the US government has an opportunity and responsibility to reinforce the global Internet's positive potential by better protecting the submarine cables that underpin it. A different future is possible, one where security and resilience are more central decision factors in the design, construction, and maintenance of undersea cables; where the US government works more proactively with industry, allies, and partners to ensure the global Internet runs reliably and securely, even in the face of failure; and where robust security for core Internet architecture is itself a compelling alternative to authoritarian visions of a state-controlled sovereign network. The US government should seize on this opportunity and embrace this responsibility.

Introduction

Much of the security commentariat has lately focused the global Internet security conversation on communications technologies deemed "emerging," such as cloud computing infrastructure, new satellite technology, and 5G telecommunications. However, the vast majority of international traffic traversing the Internet each day, from video calls to banking transactions to military secrets, travels over a much older and far less flashy technology: undersea cables.[1] These cables, which lay along the ocean floor and haul data intercontinentally, have been developed for 180 years by private sector firms and international consortia of companies. In recent years, large Internet companies (e.g., Facebook, Google) have gained significant ownership in these cables. Chinese state-owned firms have also greatly increased both their construction (e.g., Huawei Marine) and ownership (e.g., China Telecom, China Unicom) of undersea cables in recent years.

The undersea cables that carry Internet traffic around the world are an understudied and often underappreciated element of modern Internet geopolitics, security, and resilience. It is estimated that upwards of 95 percent of intercontinental Internet traffic is carried over these cables.[2] Without them, the Internet would not exist as it does today. These cables are largely owned by private companies, often in partnership with one another, though some firms involved in cable management are state-controlled or intergovernmental. Submarine cables are, therefore, a major vector of influence that companies have on the global Internet's shape, behavior, and security.[3]

Not only does the private sector manage large swaths of the constituent networks that compose the broader Internet, it also builds, owns, manages, and repairs the underlying physical infrastructure. Undersea cables are the basis of global digital interconnectedness, defining which areas of the world are connected, how those areas are connected (e.g., speed, bandwidth), and who controls those connections (e.g., the companies building the cables, the companies managing the "landing points" that link the cables to shore). Companies directing the deployment of undersea cables, therefore, produce geopolitical effects on Internet connectivity and everything that comes with it, including scientific research, digital trade, and government and personal communications. They also reshape the Internet's physical topology in the process.

Securing this physical backbone of the global Internet against damage, manipulation, and disruption has long been a vital job of the companies that own and manage this infrastructure. Yet three trends are making the security and resilience of undersea cables a more urgent issue for the US government, its allies and partners around the world, and the companies that own and manage the infrastructure. First, authoritarian governments, especially in Beijing, are reshaping the Internet's physical layout through companies that control Internet infrastructure, to route data more favorably, gain better control of internet chokepoints, and potentially gain espionage advantage. Second, more companies that manage undersea cables are using network management systems to centralize control over active components (such as reconfigurable optical add/drop multiplexers (ROADMs) and robotic patch bays in remote network operations centers), which introduces new levels of operational security risk. Third, the explosive growth of cloud computing has increased the volume and sensitivity of data crossing these cables. Some of these trends have greater effects on geopolitics and others on operations, but they are inextricably intertwined.

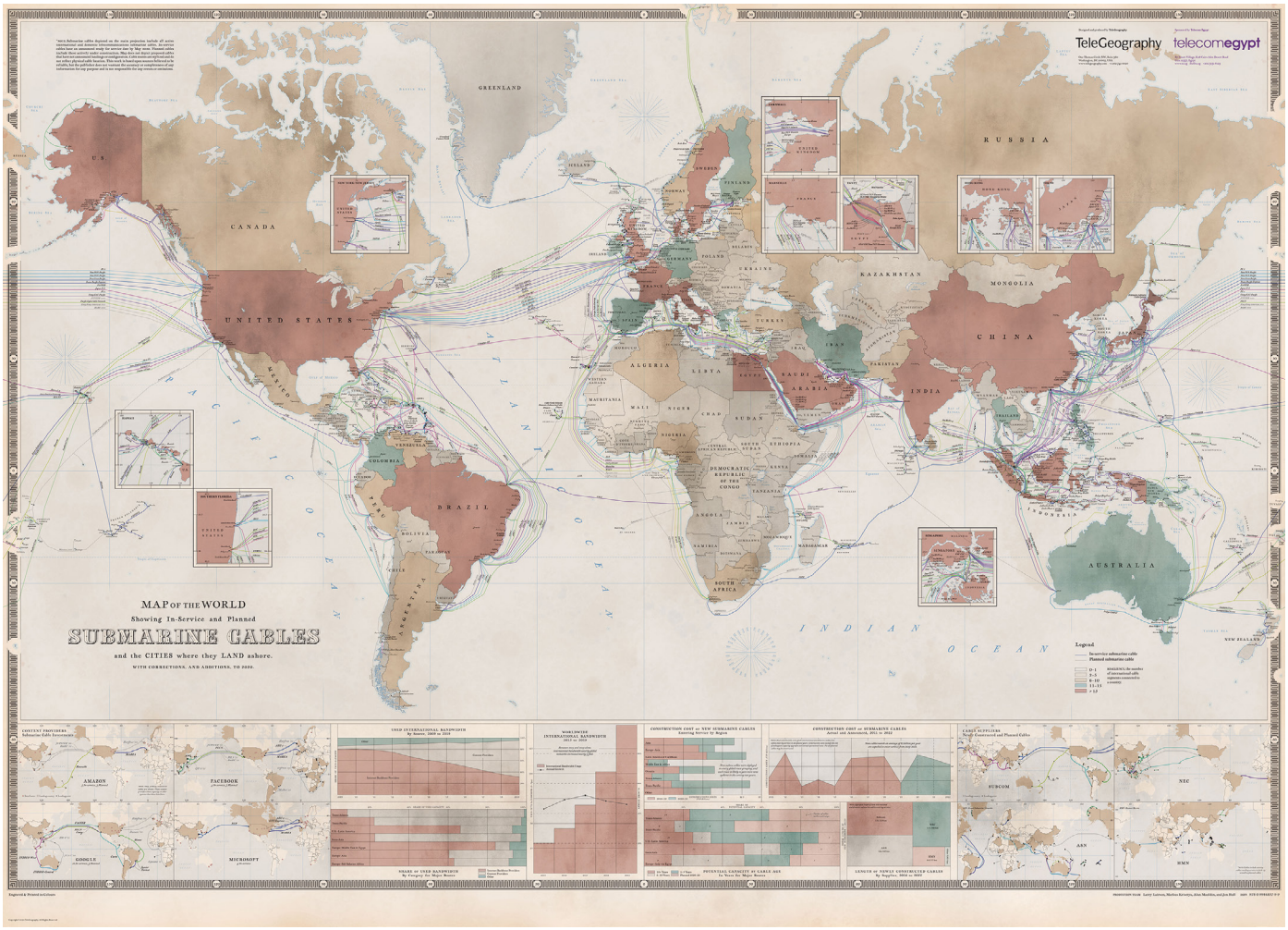
As the White House increasingly focuses on cybersecurity threats to the nation and the global community, including from the Chinese and Russian governments, it must prioritize investing in the security and resilience of the physical infrastructure that underpins Internet communications. US technology policy on China that focuses purely on 5G neglects the most central part of the global Internet infrastructure and the ways in which Beijing is reshaping and potentially dominating it. Engagement with Russia on security issues must likewise include Moscow's activities vis-à-vis monitoring undersea cables. And for all that US society may invest in securing digital systems, the cables that carry those systems' data and services remain vulnerable to surveillance, signal manipulation, and even serious damage or other disruption. Some of these issues may be addressed in forthcoming executive actions on cyber defense and supply chain security, but a comprehensive response to these threats cannot and will not be addressed by executive orders alone.

1 "Undersea cables" and "submarine cables" are used interchangeably in this report.

2 Based on conversations with US government officials. See also: "Submarine Cables," National Oceanic and Atmospheric Administration Office of General Counsel, accessed June 21, 2021, https://www.gc.noaa.gov/gcil_submarine_cables.html.

3 For background on this argument, see Justin Sherman, *The Politics of Internet Security: Private Industry and the Future of the Web*, *Atlantic Council*, October 5, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-politics-of-internet-security-private-industry-and-the-future-of-the-web/.

Image 1: TeleGeography 2020 Submarine Cable Map



Source: Jayne Miller, "The 2020 Cable Map Has Landed," *TeleGeography Blog*, June 16, 2020, https://blog.telegeography.com/2020-submarine-cable-map.

The US government, therefore, has a new opportunity and responsibility—in coordination with the US private sector and with allies and partners abroad—to significantly increase its involvement in protecting the security and resilience of undersea cables. This report makes this argument drawing on policy and technological research, interviews with key stakeholders, and empirical data collected and subsequently analyzed on the 475 undersea cables deployed around the world (at the time of writing). It is laid out as follows:

- The first chapter provides background on undersea cables and details their geopolitical importance.
- The next chapter uses empirical data on the 475 undersea cables deployed around the world, and their collective 383 owning entities, to highlight the state of Internet cable development.
- The third, fourth, and fifth chapters each examine a key trend with undersea cables: authoritarians reshaping the Internet's topology and behavior through companies; cable owners using remote management systems for cable networks; and the increasing volume and sensitivity of data sent over undersea cables. Each of these sections discusses evidence of the trend, its implications on strategic and/or operational levels, and previews of recommendations for the US government to address problems at hand.
- The final chapter concludes with eight specific recommendations for the US government to better protect the security and resilience of undersea cables in coordination with the US private sector and with allies and partners around the world.

Primer: Undersea Cable Development Today

Undersea cables vary in thickness from about 1 cm to about 20 cm, with cost-per-length roughly proportional to cross-sectional areas. Cables can be constructed in many ways, but most consist of a central strengthening member, which prevents kinking of the fiber strands, surrounded by the jacketed strands themselves, buffered in gel; then any copper cables needed to transmit power for repeaters and branching units; layers of armor; and, finally, an outer membrane intended to prevent seawater and plant and animal intrusion.[4] It is only that hair-thin inner fiber that transmits Internet data across the cable, whether emails, videos, or sensitive documents.

Fiber-optic cables are faster and cheaper than satellite communications.[5] These cables are laid across the ocean floor to connect disparate land masses, like South America and Europe. Every undersea cable also has at least two "landing points," or the locations where the cable meets the shoreline. Facilities at these landing points can provide multiple functions, including terminating an international cable, supplying power to the cable, and acting as a point of domestic and/or international connection.[6] The owner of an undersea cable (ownership is discussed more in later chapters) may not be the same entity as the owner of the landing station. As an example of this infrastructure, Image 2 depicts an undersea cable that carries Internet traffic underwater between two land masses.

For nation-states, tapping into cables carrying information around the world is an attractive spying opportunity. Back in the late nineteenth century, British intelligence used its access to an international hub of telegram cables in the small village of Porthcurno to gain eavesdropping advantage.[7] In the 1970s, the US National Security Agency deployed submarines and divers to attach recording devices

Image 2: Undersea Cable Illustration

Source: iStock

4 Thanks to Bill Woodcock, executive director of Packet Clearing House, for discussion of these details.

5 Nicole Starosielski, "In our Wi-Fi world, the internet still depends on undersea cables," *Conversation*, November 3, 2015, https://theconversation.com/in-our-wi-fi-world-the-internet-still-depends-on-undersea-cables-49936.

6 United Nations International Telecommunication Union, "Cable Landing Stations: Building, Structuring, Negotiating and Risk," 2, 2017, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Submarine%20Cable/submarine-cables-for-Pacific-Islands-Countries/Cable%20Landing%20Stations%20SNCC.pdf.

7 Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 16-17.

History of Undersea Cables

Undersea cables have been in use worldwide for decades upon decades. The first submarine cables were used in the 1820s by an attaché to the Russian Embassy in Munich to send electric telegraph communications.[1] This undersea cable technology evolved with more sophisticated telegraph communications in the mid- and late 1800s (with the first trans-Atlantic submarine telegraph cable in 1858), voice communications in the early to mid-1900s, and fiber-optic data transmission in the mid- to late 1900s.[2] Undersea cable lines were also tied with European imperial expansion and colonialism, thought of as enabling wider boundaries of global empire.[3] Today, these cables transmit previously inconceivable volumes and kinds of data, from business communications and scientific research to personal messages and military documents, making their security (confidentiality, integrity, and availability) and their resilience (the degree to which they can be restored or repaired in the event of damage or disruption) a key part of securing the global Internet in the twenty-first century.

1 Lionel Carter, Douglas Burnett, Stephen Drew, Graham Marle, Lonnie Hagadorn, Deborah Bartlett-McNeil, and Nigel Irvine, *Submarine Cables and the Oceans: Connecting the World* (Cambridge, UK: United Nations Environment Programme World Conservation Monitoring Centre, 2009), 11.

2 Ibid., 14-15; Geoff Huston, "At the bottom of the sea: a short history of submarine cables," APNIC, February 12, 2020, https://blog.apnic.net/2020/02/12/at-the-bottom-of-the-sea-a-short-history-of-submarine-cables/; Allison Marsh, "The First Transatlantic Telegraph Cable Was a Bold, Beautiful Failure," *IEEE Spectrum*, October 31, 2019, https://spectrum.ieee.org/tech-history/heroic-failures/the-first-transatlantic-telegraph-cable-was-a-bold-beautiful-failure.

3 Roxana Vatanparast, "The Infrastructures of the Global Data Economy: Undersea Cables and International Law," *Harvard Law International Journal* 61 (2020): 4-5, https://harvardilj.org/wp-content/uploads/sites/15/Vatanparast-PDF-format.pdf.

to a vulnerable cable on Russia's eastern coast that carried sensitive Russian military communications.[8] Today, a similar phenomenon occurs with undersea cables hauling Internet traffic—they are a potential information gold mine for governments. When Russia illegally annexed Crimea in 2014, the Russian military targeted the undersea cables "linking the peninsula and the mainland" to gain "control of the information environment."[9] The Russian government broadly recognizes the strategic value of physical Internet infrastructure. In December 2019, Taiwan claimed Beijing was backing private investment in Pacific undersea cables as a mechanism for spying and stealing data.[10] And the US government earlier this year paused a Google project to build an Internet cable from the United States to Hong Kong: it was concerned Beijing could use its new national security law to access cable data on the Hong Kong side.[11] Across these and other cases, access to and influence over undersea cables can have direct effects on economic and national security.[12]

Damaging these cables is another way to disrupt Internet communications. For all the intangible-sounding imagery around the Internet—"cloud," "cyberspace"—the Internet still relies on physical things to run,[13] and those physical objects, including cables, can be destroyed.[14] In 2008, a ship which tried to moor off the Egyptian coast accidentally severed an undersea cable, leaving seventy-five million people in the Middle East and India with limited Internet access.[15] In 2015, the Yemeni government shut down Internet connectivity in the country, an act of repression aided by the low bar of controlling access to just two undersea cables running into the country.[16] Even natural

8 Matthew Carle, "Operation Ivy Bells," Military.com, accessed January 2, 2021, https://www.military.com/history/operation-ivy-bells.html; Olga Khazan, "The Creepy, Long-Standing Practice of Undersea Cable Tapping," *Atlantic*, July 16, 2013, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

9 Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (New York: Routledge, 2019), 75.

10 David Brennan and John Feng, "Taiwan Says China Wants to Spy on Nations, Steal Data Through Undersea Cable Networks," *Newsweek*, December 18, 2020, https://www.newsweek.com/taiwan-china-spy-nations-steal-data-undersea-cable-networks-kiribati-connectivity-project-1555849.

11 Justin Sherman, "The US-China Battle Over the Internet Goes Under the Sea," *WIRED*, June 24, 2020, https://www.wired.com/story/opinion-the-us-china-battle-over-the-internet-goes-under-the-sea/.

12 See, for example, Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, 63, March 2016, https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

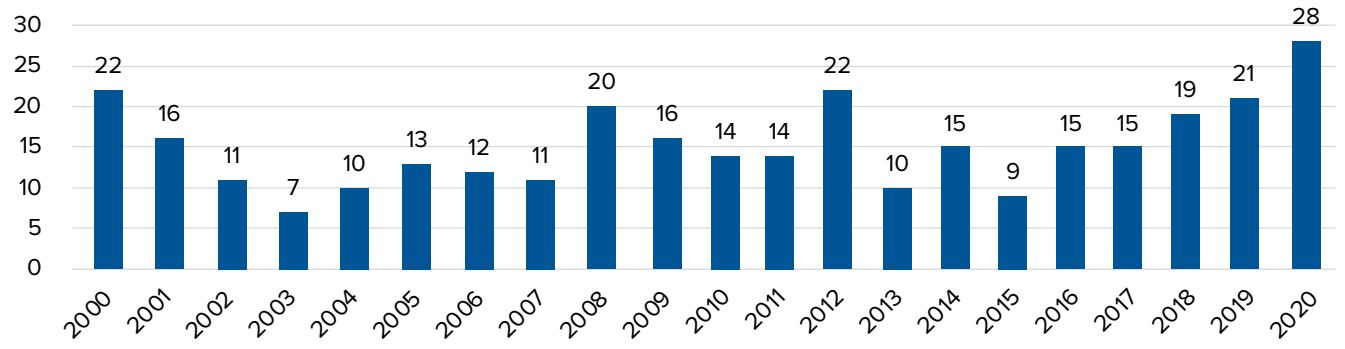
13 For more on this, see Sherman, *The Politics of Internet Security*; Robert Morgus and Justin Sherman, The Idealized Internet vs. Internet Realities (Version 1.0), New America, last updated July 26, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/.

14 Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 128.

15 Bobbie Johnson, "How one clumsy ship cut off the web for 75 million people," *Guardian*, February 1, 2008, https://www.theguardian.com/business/2008/feb/01/internationalpersonalfinancebusiness.internet.

16 Andrea Peterson, "Another casualty in Yemen: Internet stability," *Washington Post*, April 2, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/04/02/another-casualty-in-yemen-internet-stability/.

Figure 1: Cables Ready for Service per Year, Global (2000-2020)



Source: Data from TeleGeography's Submarine Cable Map website visualized by author.

weather events like undersea earthquakes can damage cables and temporarily decrease Internet availability to an entire region.[17] Ensuring the resilience of undersea cables—that they help route data around failure and are quickly restored if damaged or disrupted—is thus critical to ensuring the resilience of global Internet traffic and the societal functions that depend on it. This is not to say that a single damaged cable will bring down the global Internet, for the Internet is designed to route around failure, and data can be sent via other routes, though it could substantially decrease Internet connectivity for a country or region.[18] There are also not many publicly documented examples of governments destroying or damaging cables, even though there is much national security concern about the potentially severe consequences should governments elect to pursue those ends (e.g., in a wartime scenario).[19] But ensuring submarine cable resilience, especially for key chokepoints in the global network, is geopolitically important because even slow repairs of major cables can slow down traffic delivery between land masses.

For all undersea cables' implications for governments, the private sector's involvement comes into play with each of the aforementioned activities, from intelligence collection to damage repair. Governments looking to spy on the data traveling across submarine cables often turn to private sector companies to carry it out because the private sector has a heavy involvement in cable ownership and maintenance worldwide. Citizens, businesses, and government agencies who need Internet access restored after a submarine cable is damaged likewise often turn to the private sector to repair the infrastructure and restore Internet connectivity. More broadly, on the geopolitical level, governments looking to improve the security of physical Internet infrastructure, or those looking to alter the global Internet's physical shape and digital behavior in their image, must include the private sector's influence on undersea cables in their strategies and policies because those firms often directly control and deeply understand the infrastructure. This has been true for much of the critical infrastructure in democracies, and specifically with telecommunications cables, for some time.

There are 475 of these undersea cables deployed around the world as of December 2020. This number and this report's analysis of those cables draws on a compilation of publicly available data from TeleGeography's Submarine Cable Map website, coded with additional data gathered from open sources on the 383 different entities (private firms and state-controlled entities) with listed ownership stakes in those cables.[20] The first observation from this data is that cable development, globally, is on the rise. Figure 1 shows the number of undersea cables ready for service—that is, fully built and ready to be used—around the world from 2000 to 2020.

By these numbers, the rate of submarine cable deployment is increasing. In 2016, fifteen new cables were ready for service around the world. In 2020, twenty-eight new cables entered service around the world, representing an

17 Dante D'Orazio, "Into the Vault: The Operation to Rescue Manhattan's Drowned Internet," *Verge*, November 17, 2012, https://www.theverge.com/2012/11/17/3655442/restoring-verizon-service-manhattan-hurricane-sandy.

18 See, for example, Louise Matsakis, "What Would Really Happen If Russia Attacked Undersea Internet Cables," *WIRED*, January 5, 2018, https://www.wired.com/story/russia-undersea-internet-cables/.

19 Most damage is caused by natural disasters and accidents.

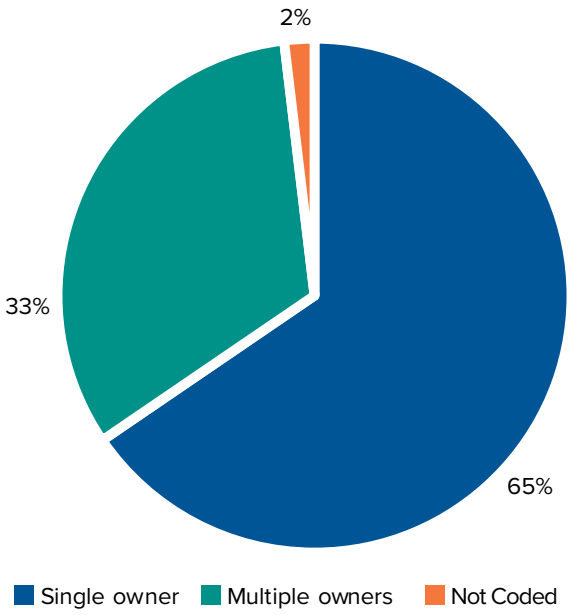
20 Data on the 475 undersea cables deployed worldwide were pulled from the publicly accessible TeleGeography Submarine Cable Map (https://www.submarinecablemap.com/) as of December 2020. Data on the 383 entities that collectively have listed ownership stake in those cables were also pulled from the Submarine Cable Map site (as of December 2020), and then coded as privately or state-owned using open sources (including stock listings, regulatory disclosures, the entities' websites and public documents, and media reporting).

almost twofold increase in just four years. This uptick is no accident—there are several drivers at play. More traffic is sent over the global Internet every year (discussed further in the third trends chapter). More countries are also looking to expand Internet penetration within their borders (e.g., how many people have Internet access) as well as to expand the bandwidth available to those Internet users.[21] Cloud service providers are getting more involved in directing the building of physical infrastructure to support their data storage and routing services. And broadly, Internet companies can also profit off cable investments in the long run by using this physical infrastructure to push their own data across the global Internet more quickly.[22]

This global Internet infrastructure has long been developed by an international consortia of companies. One single cable may have several corporate owners, often each incorporated in different countries. This consortium-based approach to cable construction and maintenance is driven by a variety of factors, including the financial costs[23] and complex logistics of laying cables across the ocean floor, the number of shorelines those cables may touch (and, therefore, the need to have a company at the other end to manage a landing point), and the profit those companies can generate from hauling cable traffic. For instance, the Europe India Gateway cable, a 15,000-km-long cable put into operation in February 2011, connects eleven different countries and has sixteen different co-owners, ranging from AT&T (the United States) to Djibouti Telecom (Djibouti) to Airtel (India) to Vodafone (the United Kingdom). The Japan-Guam-Australia South Cable System, to give a recent example, went operational in March 2020, connects Australia and the United States, and is owned by Google (the United States), RTI Cables (the United States), and Australia's Academic and Research Network (Australia; a nonprofit company originally set up by Australian universities).[24] Each one of the deployed cables is unique based on such factors as length, bandwidth, and the number of shorelines on which it lands.

Not all submarine cables have multiple owners, but this international collaboration between different firms is a key component of financing their construction and subsequently maintaining them. Figure 2 illustrates the number of cables deployed around the world with different numbers of owners.

Figure 2: Cables With Single vs. Multiple Owners (December 2020 Snapshot)



Source: Data from TeleGeography's Submarine Cable Map website visualized by author.

Mapping the ownership landscape of submarine cables is critical to understanding what levers of control can be pulled by private companies, state-owned firms, and governments. While some parts of the Internet's physical and digital infrastructure are maintained by a few core private sector companies,[25] these cables are different. The majority of undersea cables deployed worldwide—65 percent

21 See, for example, Cisco, *Cisco Annual Internet Report* (2018-2023), 2020, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf; and on digital divides worldwide, Jan A.G.M. van Dijk, Closing the Digital Divide: The Role of Digital Technologies on Social Development, Well-Being of All and the Approach of the Covid-19 Pandemic, United Nations, July 2020, https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/07/Closing-the-Digital-Divide-by-Jan-A.G.M-van-Dijk-.pdf; Internet Society, 2017 Internet Society Global Internet Report: Paths to Our Digital Future, 2017, https://future.internetsociety.org/2017/wp-content/uploads/sites/3/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf.

22 Klint Finley, "How Google Is Cramming More Data Into Its New Atlantic Cable," *WIRED*, April 5, 2019, https://www.wired.com/story/google-cramming-more-data-new-atlantic-cable/.

23 This often ranges from tens to hundreds of millions of dollars. See, e.g., *Submarine Cable Almanac* 33 (February 2020), https://issuu.com/subtelforum/docs/almanac_issue_33.

24 Submarine cable data compiled from TeleGeography's Submarine Cable Map website.

25 For instance, the global cloud computing infrastructure is dominated by the US "hyper-scalers" Microsoft, Google, and Amazon. Within any given 4G cellular network, there is usually only a single cellular supplier (e.g., Vodafone, AT&T) with predominant ownership of the infrastructure. See, for example, Trey Herr, *Four Myths About the Cloud: The Geopolitics of Cloud Computing, Atlantic Council*, August 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing/; Dana Mattioli and Aaron Tilley, "Amazon Has Long Ruled the Cloud. Now It Must Fend Off Rivals," *Wall Street Journal*, January 4, 2020, https://www.wsj.com/articles/amazon-has-long-ruled-the-cloud-now-it-must-fend-off-rivals-11578114008.

as of December 2020— have a single owner. Only a third of deployed cables have multiple owners. Within that latter category, those ownership structures are themselves varied. Seventy-two cables have just two owners, twenty-one cables have just three owners, and fifteen have four owners. These numbers are higher in some cases, though: four cables each have eighteen owners spanning several countries, and the highest number of owners for any single cable is fifty-three—the 39,000-km SeaMeWe-3 cable deployed in September 1999. The cables with multiple owners are often the ones that cost more to build and maintain, such as those connecting more countries and with higher bandwidth. Such consortia may also involve a state-controlled firm.

The distinction of the number of owners is important from a security and resilience perspective because it can produce a diversity of control over cables, it can produce a situation where multiple governments have legal oversight over companies involved with building and/or maintaining a single cable, and it can make more difficult the process of determining which entities have control over a cable and to what extent that creates risks to infrastructure.

Three trends are increasing security and resilience risks to submarine cables. As a result, there is an accentuated opportunity and responsibility for the US government to work more effectively with allies, partners, and private companies to better protect their security and resilience. These three motivating trends are each discussed in the following chapters: first, authoritarian governments reshaping the Internet's physical topology and digital behavior through companies, to route data more favorably, gain better control of internet chokepoints, and potentially gain espionage advantage; second, companies using remote management systems for cable networks, introducing new levels of cybersecurity risk; and third, the growing volume and sensitivity of data sent over these cable systems.

Trend 1: Authoritarian Governments Reshaping the Internet through Companies

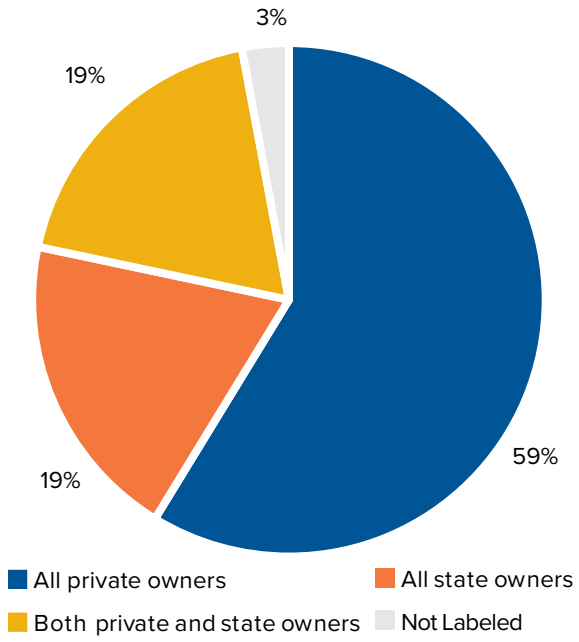
Authoritarian governments are increasingly reshaping the Internet's physical topology (structure) and digital behavior by exerting control over companies. This accelerates security and resilience risks to undersea cables because authoritarian governments—particularly in Beijing and Moscow—can use that control to undermine Internet security and resilience, and favorably shape the topology of the Internet itself, for their own strategic purposes. For instance, this could include the Chinese government building cables that will increase the overall flow of Internet traffic through its borders, which it could then exploit for intelligence gathering. Certainly, building more cables in and of itself, in a sense, arguably increases the resilience of the global Internet in absolutist terms: there are new routes over which data can travel in the event of failure. But if authoritarian governments have increasing influence over submarine cables globally, that creates its own risks of those governments manipulating and disrupting the infrastructure.

States must go through companies, in many cases, to reshape the Internet's topology. This is because much of the global Internet infrastructure is in companies' hands (even if some of those companies are state-controlled), as depicted in Figure 3.

The majority (59 percent) of global undersea cables deployed as of December 2020, or 279 out of 475 cables, have only private owners. The worldwide private sector is thus influential not just on the Internet's digital rules but also on its changing physical shape. By contrast, only 19 percent of all cables deployed worldwide, or ninety-three out of 475, are entirely owned by state-controlled entities (e.g., owned directly by a government or through a subsidiary).[26] Of course, ownership by a private firm does not mean that a government cannot directly or indirectly exert control over a cable. For example, the US government, as with most others, has a long history of tapping into private sector-controlled Internet infrastructure for espionage purposes. In most liberal democracies, however, factors such as rule of law and oversight and accountability mechanisms for surveillance place controls on the degree to which the government can influence that infrastructure. By contrast, many authoritarian regimes do not have those same oversight mechanisms and the same independence between the state and the private sector. Understanding a cable's ownership structure is still important for assessing state influence on the submarine cable network.

The Chinese and Russian governments are increasingly working to reshape the Internet through control over companies. This matters on the geopolitical level for Internet security and resilience because choosing where, when, and how to build cables is a way to shape where global Internet traffic is routed.[27] Changes to traffic routing patterns generate profits for companies and can move new volumes of traffic through different countries' borders.

Figure 3: Cables' Public-Private Ownership Breakdown (December 2020 Snapshot)



Source: Data from TeleGeography's Submarine Cable Map website visualized by author.

26 For this report, companies coded as "state-controlled" were those either directly, majority owned by a national government or indirectly, majority owned by a subsidiary of a national government (e.g., majority owned by another state-owned company). Public companies in which the national government is a minority shareholder, for instance, and public companies in which multiple local governments are shareholders were not in this classification.

27 This is reflected in the fact that "traffic that appears to be traveling via separate network paths could potentially be relying on the same physical resource." Zachary S. Bischof, Romain Fontugne, and Fabián E. Bustamante, "Untangling the world-wide mesh of undersea cables," HotNets '18: Proceedings of the 17th ACM Workshop on Hot Topics in Networks, 81, November 2018, https://dl.acm.org/doi/abs/10.1145/3286062.3286074.

This can enable data interception and the development of technological dependence. Yet these geopolitical influences also affect the operational level of securing undersea cables. Cable owners might insert backdoors into or otherwise monitor landing stations. Cable builders might similarly compromise the security of the physical infrastructure along the ocean floor before it is laid. As Beijing and Moscow exert more control over Internet companies, the risk of them undermining Internet security and resilience grows. This trend also connects with the other two key trends discussed later in the report: the growing cybersecurity vulnerability of cable networks and the more sensitive data sent over cables create larger incentives for states to intercept that information.

The Russian government has increasingly exerted control over companies with influence on Internet infrastructure to serve geopolitical purposes. For decades, the Kremlin has spoken of the importance of state control of the Internet, and that has included Internet infrastructure. In 2011, for example, then Russian president Dmitry Medvedev told G20 leaders that Internet infrastructure needed more state regulation to account for the "public interest."[28] In 2014, as Russia was illegally annexing Crimea, there were reports of armed men damaging fiber-optic cables that carried Internet traffic to Ukraine.[29] Finnish media have reported on alarm over Russian land acquisitions beyond Russia that are in the vicinity of key telecommunications links, such as around the Turku archipelago.[30] In 2017, Andrew Lennon, then commander of NATO's submarine forces, told the *Washington Post* that "we are now seeing Russian underwater activity in the vicinity of undersea cables that I don't believe we have ever seen" and that "Russia is clearly taking an interest in NATO and NATO nations' undersea infrastructure."[31] The 2021 Office of the Director of National Intelligence's unclassified threat assessment found that Russia "continues to target critical infrastructure, including underwater cables."[32] And broadly, the Kremlin continues expanding its control over domestic technology firms to serve and protect its political agenda.[33]

Rostelecom, the Russian state-owned telecommunications giant, is a prime example of a firm whose influence on Internet infrastructure seems to be continually leveraged by the Kremlin. Data compiled for a previous report showed Rostelecom to be involved with dozens of potential hijacks of the Border Gateway Protocol (BGP), the Internet's "GPS" for traffic, in the first few months of 2020 alone; it appeared the company deliberately rerouted reams of global Internet traffic through Russian borders, a tactic used by several authoritarian governments to spy on Internet data.[34] This practice weaponizes a security flaw at the very core of the global Internet.

In an August 2020 meeting, meanwhile, Rostelecom President Mikhail Oseyevsky told Russian President Vladimir Putin that the company was "completing an ambitious basic infrastructure expansion programme in the Far East," having recently laid cables to Russian islands. Oseyevsky added that Rostelecom saw "additional opportunities for working on international markets" in light of rising global volumes of Internet traffic, a situation in which "Russia can provide the simplest and most reliable method for transmitting these volumes from Europe to Asia."[35] This is significant because Rostelecom is a state-owned firm, and all such "meetings" with Putin are scripted. Thus, in addition to the likely security dimensions of Russia's Internet infrastructure foothold, it also appears to have economic dimensions—with submarine cables serving as a potential mechanism for the Kremlin to grow its levers of economic coercion.

The Chinese government also presents risks in this vein across cable ownership and cable construction. Broadly, numerous governments, researchers, and independent observers have expressed concerns about the Chinese government's exerted influence over technology companies within its borders. Domestically, the Chinese government's Internet filtering and surveillance regime depends on the cooperation of private companies that own and manage the infrastructure.[36] It is these firms that may set

28 Kremlin.ru, "Dmitry Medvedev's message to the G20 leaders," November 3, 2011, http://en.kremlin.ru/events/president/news/13329.

29 Pavel Polityuk and Jim Finkle, "Ukraine says communications hit, MPs phones blocked," Reuters, March 4, 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304.

30 Keir Giles, "The Next Phase of Russian Information Warfare," NATO Strategic Communications Centre of Excellence, 12, May 20, 2016, https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

31 Michael Birnbaum, "Russian submarines are prowling around vital undersea cables. It's making NATO nervous," *Washington Post*, December 22, 2017, https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?utm_term=.a57f9e4f495f.

32 Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, 10, April 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

33 Dylan Myles-Primakoff and Justin Sherman, "Russia's Internet Freedom Shrinks as Kremlin Seizes Control of Homegrown Tech," *Foreign Policy*, October 26, 2020, https://foreignpolicy.com/2020/10/26/russia-internet-freedom-kremlin-tech/.

34 These incidents were particularly suspicious as Rostelecom has been involved in numerous such attacks before. See Sherman, *The Politics of Internet Security*.

35 Kremlin.ru, "Meeting with Rostelecom President Mikhail Oseyevsky," August 5, 2020, http://en.kremlin.ru/events/president/news/63857.

36 For more on this regime, see Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018).

Figure 4: Risk Overview of Chinese State Influence through Cable Owner vs. Cable Builder

State influence via...	The company:	The risks:	Some Chinese firms in question:
Cable owner	Owns and maintains, and may have financed, the cable	Spying on data, disrupting data, shaping cable layout	China Mobile, China Telecom, China Unicom
Cable builder	Builds part of the cable (such as the fiber or the cable itself)	Backdooring equipment	Huawei Marine

Source: Visualized by author.

up state-mandated filtering technologies on their Internet hardware or build algorithms to flag certain keywords on their digital platforms.[37] Similarly, there are concerns that the Chinese government exerts that same kind of control over foreign-operating Chinese companies to reshape the Internet's physical topology and digital rules. Chinese state-owned firms have (akin to Rostelecom) been involved with repeated hijackings of the BGP, where global Internet traffic is rerouted through Chinese borders, over the last few years.[38]

There are real risks that Chinese state-owned Internet companies that own or manage Internet infrastructure will become vectors for the government to reshape the Internet's topology and behavior. There are also concerns that Chinese government capacity-building projects abroad have involved building computer systems that secretly exfiltrate data to Beijing.[39] Two specific risks of Chinese government influence over cable-involved companies—influence through a cable owner and influence through a cable builder—form the basis of a more detailed case study below.

Risk 1: Chinese State Influence through Cable Owner

First, there is a risk of Chinese government influence through the (co-)owner of a cable, which is typically involved in funding the construction of the cable from the beginning. This risk implicates Internet security and resilience because faster routes for Internet data are generally preferable to slower ones.[40] Cable investors can, therefore, shape the flow of global Internet traffic by choosing the connecting nodes and the bandwidth of new undersea cables: as the Internet's physical shape changes, offering newer and faster routes for data between locations, more data could get digitally routed along different paths and through different countries' borders. Infrastructure changes, in other words, affect the Internet's digital behavior—potentially increasing economic dependence and enabling traffic interception. Cable owners with control of landing stations could also provide an intelligence collection vector for governments who mandate the insertion of monitoring equipment or backdoors. States exerting more control over cable owners thus creates impacts on Internet security and resilience, on both geopolitical and operational levels.

The US government, as previously mentioned, recommended in June 2020 that the Federal Communications Commission (FCC) refuse to approve cable licensing for the Pacific Light Cable Network (PLCN)—a submarine cable involving Google, Facebook, a New Jersey-based telecom, and a Hong Kong-based telecom owned by a Chinese firm—because its routing of US data through Hong Kong allegedly posed a national security risk. One of the Department of Justice's (DOJ's) specific concerns was that Beijing would use the Chinese owner of the Hong Kong subsidiary to access data on US persons. It cited "the current national security environment, including the PRC government's sustained efforts to acquire the sensitive data of millions of U.S. persons" as well as the cable

37 See, for example, Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, *Censored Contagion: How Information on the Coronavirus is Managed on Chinese Social Media*, Citizen Lab, March 3, 2020, https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.

38 Sherman, The Politics of Internet Security.

39 Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," ("In Addis Ababa, the headquarters of the African Union spied on by Beijing"), *Le Monde*, January 27, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

40 Quicker routes for Internet data are not always chosen, but they are generally preferred to slower ones.

Figure 5: Cables Owned by Chinese State-Controlled Entities (December 2020 Snapshot)

Entity	Ownership by Chinese Government	Number of Sole-owned Cables	Number of Co-owned Cables
China Mobile	State-owned	1	10
China Telecom	State-owned	0	15
China Unicom	State-owned	0	12
CITIC Telecom International	State-controlled	0	1
CTM	State-controlled	0	1
National Grid Corporation of the Philippines	Beijing is a consortium member	0	1

Source: TeleGeography's Submarine Cable Map.

project's "connections to PRC state-owned carrier China Unicom" as reasons for blocking the cable's development. The DOJ also cited:

> "Concerns that PLCN would advance the PRC government's goal that Hong Kong be the dominant hub in the Asia Pacific region for global information and communications technology and services infrastructure, which would increase the share of U.S. internet, data, and telecommunications traffic to the Asia Pacific region traversing PRC territory and PRC-owned or -controlled infrastructure before reaching its ultimate destinations in other parts of Asia."[41]

In other words, the US government highlighted the risk of Chinese state influence on two fronts: compromising cable data via cable owners (e.g., intelligence collection through a state-controlled landing point) and changing the Internet's physical shape to route more global traffic through China (e.g., creating more chokepoints in the global network under the Chinese government's control). These risks are distinct but related, as the referenced actions can be carried out by the same entity.

The DOJ is not alone in its concerns about the Chinese government's control of cable owners. In November 2019, CNN reported on an internal Filipino government report alleging that the National Grid Corporation of the Philippines, partly owned by a Chinese state-owned electrical company, was in fact "under the full control" of the Chinese government and vulnerable to disruption.[42] Reporting focused on the Filipino power grid, but the National Grid Corporation of the Philippines is also the sole owner of an undersea cable in the Philippines, making the Chinese state firm a co-owner.[43] If those concerns about disruption apply to the power grid, there are related questions to be asked about Beijing's influence over the submarine cable. In December 2020, Taiwan accused the Chinese government of backing Pacific-area cable investments as a means of spying on foreign countries and stealing data; a spokesperson for Taiwan's Ministry of Foreign Affairs told *Newsweek* that Beijing wanted to "monopolize" Pacific information.[44] These allegations arrive as Chinese state-controlled entities are taking growing ownership stakes in undersea cables, as depicted in Figure 5.

The three Chinese-incorporated firms listed as owners of undersea cables (at the time of writing)—China Mobile,

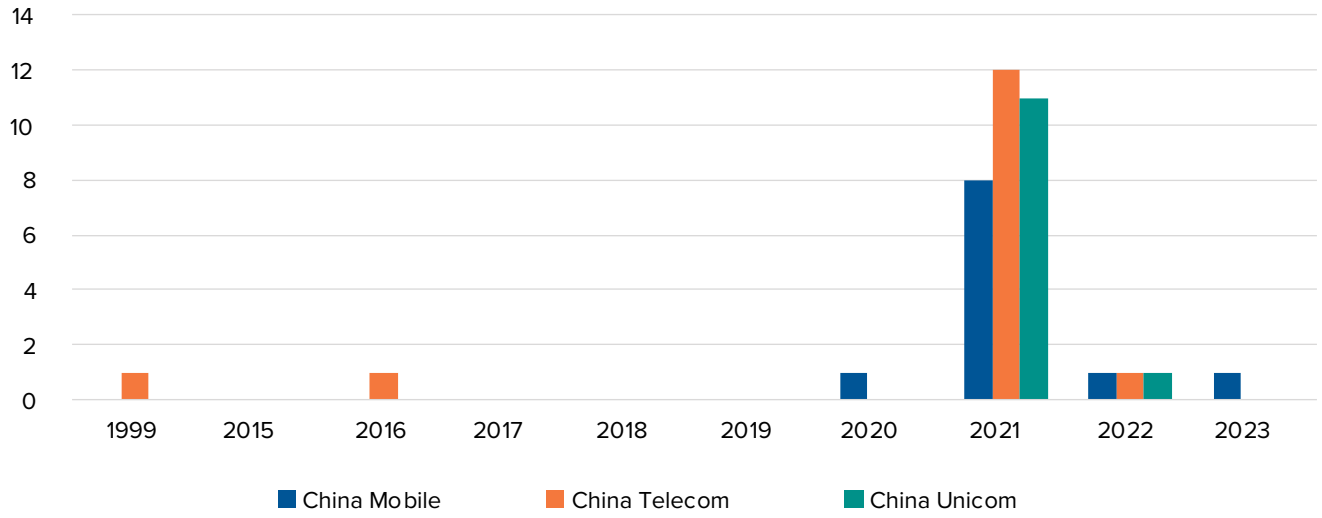
41 U.S. Department of Justice Office of Public Affairs, Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States, press release number 20-555, June 17, 2020, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

42 James Griffiths, "China can shut off the Philippines' power grid at any time, leaked report warns," CNN, November 26, 2019, https://edition.cnn.com/2019/11/25/asia/philippines-china-power-grid-intl-hnk/index.html; CNN Philippines Staff, "Carpio: Chinese 'control' of national power grid a cause for concern," CNN, November 26, 2019, https://www.cnnphilippines.com/news/2019/11/26/Antonio-Carpio-Chinese-control-NGCP.html.

43 This is the Sorsogon-Samar Submarine Fiber Optical Interconnection Project (SSSFOIP) cable deployed in 2019.

44 Brennan and Feng, "Taiwan Says China Wants to Spy."

Figure 6: Current Chinese State-Owned Telecom Cable Ownership, by Year Ready for Service (December 2020 Snapshot)



Source: Data from TeleGeography's Submarine Cable Map website visualized by author.
Note: Cables listed in the future are coded based on their expected ready-for-service date

China Telecom, and China Unicom—are all state-owned. In addition, two other companies that own cables, CITIC Telecom International and CTM, incorporated in Hong Kong and Macau, respectively, are themselves controlled by the Chinese government. The Chinese government is also a part of the aforementioned National Grid Corporation of the Philippines, a consortium of different cable owners. China Mobile, China Telecom, and China Unicom largely do not own years-old cables, however; the rate at which they are co-owners of newly deployed submarine cables is growing, as depicted in Figure 6.

The three Chinese state-owned telecoms' quickly rising investment in undersea cables increases the risk that Beijing leverages that influence to support its monitoring of cable data. It also gives the Chinese government more power to shape, quite literally, how and where cables are laid before construction even begins. For projects scheduled in 2021, China Mobile is currently invested as an owner in twenty-one, China Telecom is invested in twelve, and China Unicom is invested in eleven. On top of that, each state-owned company is invested in at least one project into 2022 or 2023. Currently, the firms have barely any stake (at the time of writing) in cables deployed before 2020, a stark departure from the many other companies around the world with ownership stakes in cables deployed back in the 1990s or early 2000s. And these firms' activity in the United States has drawn scrutiny from Washington. The FCC denied China Mobile's application to provide telecom services in the United States in 2019, citing national security risks.[45] A year later, it ordered China Telecom and China Unicom to provide evidence they did not pose national security risks through their US operations.[46]

This growing investment is also likely tied to the Chinese government's infrastructure capacity building around the world—and risks of Beijing reshaping the Internet's topology globally. Beijing is estimated to be spending hundreds of billions of dollars on infrastructure development projects in dozens of countries as part of its Belt and Road Initiative (BRI).[47] In 2015, Beijing launched its Digital Silk Road (DSR) project, formally making a focus on Internet technology and infrastructure a part of the broader BRI.[48] A 2015 white paper released by China's National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce reads, "[China] should

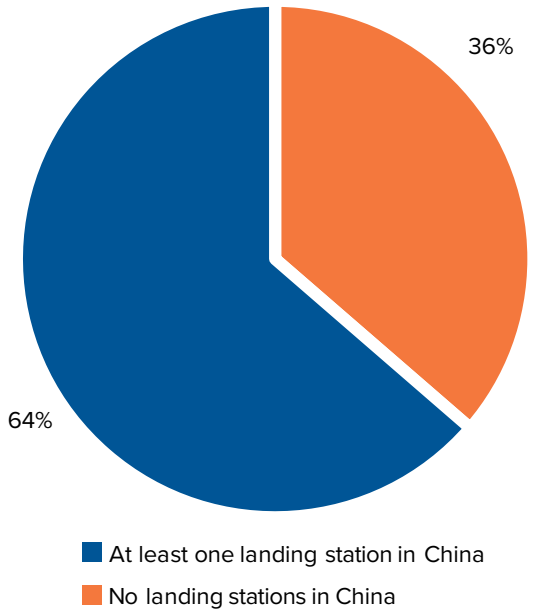
45 US Federal Communications Commission, FCC Denies China Mobile USA Application to Provide Telecommunications Services, press release, May 9, 2019, https://docs.fcc.gov/public/attachments/DOC-357372A1.pdf.

46 U.S. Federal Communications Commission, "FCC Scrutinizes Four Chinese Government-Controlled Telecom Entities," April 24, 2020, https://www.fcc.gov/document/fcc-scrutinizes-four-chinese-government-controlled-telecom-entities.

47 Andrew Chatzky and James McBride, *China's Massive Belt and Road Initiative, Council on Foreign Relations*, January 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

48 Joshua Kurlantzick, "China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom?" *Diplomat*, December 17, 2020, https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/.

Figure 7: Landing Stations of China Mobile-, China Telecom-, and China Unicom-Owned Cables (December 2020 Snapshot)



Source: Data from TeleGeography's Submarine Cable Map website visualized by author.

jointly advance the construction of cross-border optical cables and other communications trunk line networks, improve international communications connectivity, and create an information Silk Road." It also specifically mentioned planning undersea, transcontinental cable projects.[49]

These projects, when conducted by or with Chinese state-owned or -controlled firms, are a potential way for Beijing to influence the Internet's physical shape. Once the projects are completed, it is possible they could be used as economic and/or technological levers of influence. Since 2015, Chinese firms have moved to fill cable-building voids in low-resourced countries,[50] including with heavy focus on Internet infrastructure across the African content.[51] The Chinese government has also signed DSR cooperative agreements, or given DSR-linked investment to, at least sixteen countries, and dozens more BRI participants may be involved with DSR projects.[52] Not all DSR projects are directly state-controlled or -supervised to the same degree, but the Chinese government's control over specific elements of the DSR is only poised to grow in the coming years.[53] In December 2020, Chinese Foreign Minister Wang Yi claimed government spending on the BRI, digital infrastructure included, had increased in 2020 even with the COVID-19 pandemic.[54] This focus on capacity building abroad aligns with data on cables owned by Chinese state-owned firms, depicted in Figure 7.

China Mobile, China Telecom, and China Unicom collectively own twenty-two cables; there is some overlap in their cable investments. Significantly, however, many of these projects are entirely focused abroad. Figure 7 shows that more than one-third of submarine cables owned by these Chinese state-owned firms do not have landing stations in China—that is, they make no direct contact with the Chinese mainland. This is not inherently cause for concern. Many companies invest in cables that do not touch the shores of their country of incorporation because it can be a way to make money off Internet traffic as well as influence the Internet's physical shape in business-favorable ways (e.g., building faster data transmission to a new market).[55] But growing investment notably coincides with the Chinese government's focus on capacity building worldwide and its efforts to reshape the Internet's physical topology and digital behavior.

Risk 2: Chinese State Influence through Cable Builder

Second, there is a risk of Chinese government influence through the builder of a cable rather than its (co-)owner. This is an important distinction because the companies building a cable are different from the ones that fund the project and ultimately own the cable. State influence through this vector could theoretically let a government

49 Quoted in Keshav Kelkar, "From silk threads to fiber optics: The rise of China's digital silk road," Observer Research Foundation, August 8, 2018, https://www.orfonline.org/expert-speak/43102-from-silk-threads-to-fiber-optics-the-rise-of-chinas-digital-silk-road/.

50 Stacia Lee, "The Cybersecurity Implications of Chinese Undersea Cable Investment," East Asia Center at the University of Washington, February 6, 2017, https://jsis.washington.edu/eacenter/2017/02/06/cybersecurity-implications-chinese-undersea-cable-investment/.

51 It is estimated the Chinese government spent approximately $20 billion on infrastructure development across Africa in 2017, including information and communications technology. The Infrastructure Consortium for Africa, *Infrastructure Financing Trends in Africa – 2017*, 54, 2018, https://www.icafrica.org/fileadmin/documents/Annual_Reports/IFT2017.pdf.

52 Kurtlantzick, "China's Digital Silk Road Initiative."

53 Paul Triolo and Robert Greene, "Will China control the global internet via its Digital Silk Road?" SupChina, May 8, 2020, https://supchina.com/2020/05/08/will-china-control-the-global-internet-via-its-digital-silk-road/.

54 Rachel Zhang, "Belt and Road Initiative: China ups investment despite coronavirus and doubters," *South China Morning Post*, December 21, 2020, https://www.scmp.com/news/china/diplomacy/article/3114824/china-sells-confident-message-its-belt-and-road-initiative.

55 For instance, see Facebook's investment in undersea cables linked to African countries as it pursues market expansion across the continent: Ryan Browne, "Facebook is building a huge undersea cable around Africa to boost internet access in the continent," CNBC, May 14, 2020, updated June 2, 2020, https://www.cnbc.com/2020/05/14/facebook-building-undersea-cable-in-africa-to-boost-internet-access.html.

insert vulnerabilities into cables before they are even laid underwater. Evidence, as always, is vital to assessing this risk, as is the Chinese government's supposed cost-benefit calculus on information collection; the mere existence of possibility is not enough. But along with Beijing's growing leveraging of Chinese technology companies for its geopolitical interests, this second risk of state control speaks to geopolitical and operational issues: states potentially monitoring, corrupting, or disrupting the flow of data.

Any company that builds parts of cables—whether a company like Corning that makes optical fiber or a company like TE SubCom that lays a cable underwater—could potentially be tapped on the shoulder by a government to build backdoors into the equipment before deployment. There are multiple parts of the submarine cable supply chain that could each potentially be compromised in this fashion. This kind of backdooring is distinct from the many other ways in which governments could potentially tap into cables once they are deployed, from hacking into remote network management systems (discussed more in the next section) to installing physical taps on cable lines.

The Chinese company Huawei Marine has been a focus of such espionage concerns internationally. Huawei Marine has no identified ownership stake in any of the 475 undersea cables deployed worldwide as of this report's writing. The company has, however, been involved in laying numerous undersea cables, and repairing those cables, around the world. According to an October 2020 FCC document, Huawei Marine has "built or repaired almost a quarter of the world's cables."[56] Examples abound of Huawei partnering with telecoms in other countries to build undersea cables. For instance, in April 2019, Huawei announced a partnership with FiberStar, the Indonesian telecom, to "deepen cooperation in addition to building a high-speed optical fiber network." The Huawei press release also noted that Huawei had already worked with FiberStar to build an enhanced fiber-optic backbone connecting Jakarta to Surabaya.[57] This is not on its face unusual, given the private sector's influence on the bulk of global Internet infrastructure and that collaboration is a common feature of undersea cable development. The question comes down to the risk that a specific company—in this case, Huawei, one with critical foothold in global Internet architecture and alleged close ties to the Chinese government[58]—is a vector of state geopolitical influence projecting. In this case, the US government has reportedly been warning Pacific Island countries that Huawei Marine's cable-building activities pose security risks.[59]

One could argue these disputes are essentially two major powers vying for espionage advantage.[60] The Chinese state-controlled *Global Times* itself quoted a telecom industry writer in July 2019 as saying, "The US's undersea battle with Huawei is all about taking control of data and information, which is also the backbone of networks. Washington is worried that China will gain a larger stake in the submarine cable market so that Americans will not be able to listen in to networks or steal data from others."[61] The *Global Times*' propaganda purposes aside, espionage is a genuine reason for states to be concerned about information hauled over submarine cables. In 2014, for example, after the Snowden leaks about US global espionage and surveillance programs, Brazil announced plans for its own undersea cables "so that data can travel between Brazil and the European Union without going through the United States."[62] One such cable was completed in December

56 Federal Communications Commission, "Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership," 82, October 1, 2020, https://docs.fcc.gov/public/attachments/FCC-20-133A1.pdf.

57 Huawei, FiberStars Signs MoU with Huawei to Jointly Build Ultra-Broadband Network, news release, April 8, 2019, https://www.huawei.com/us/news/2019/4/huawei-fiberstar-mou-ultra-broadband-network.

58 There are many components to this debate over Huawei's ties with the Chinese Communist Party. For example, see Gordon Corera, "Huawei: MPs claim 'clear evidence of collusion' with Chinese Communist Party," BBC News, October 8, 2020, https://www.bbc.com/news/technology-54455112; Lindsay Maizland and Andrew Chatzky, *Huawei: China's Controversial Tech Giant, Council on Foreign Relations*, August 6, 2020, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant; Li Tao, "Huawei says relationship with Chinese government 'no different' from any other private company in China," *South China Morning Post*, December 26, 2019, https://www.scmp.com/tech/big-tech/article/3043558/huawei-says-relationship-chinese-government-no-different-any-other; Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736; Raymond Zhong, "Who Owns Huawei? The Company Tried to Explain. It Got Complicated," *New York Times*, April 25, 2019, https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html; Graham Webster, "Five points on the deeply flawed U.S. Congress Huawei report," TransPacifica.net, October 2012, https://transpacifica.net/2012/10/five-points-on-the-deeply-flawed-u-s-congress-huawei-report/.

59 Jonathan Barrett, "Exclusive: U.S. warns Pacific islands about Chinese bid for undersea cable project – sources," Reuters, December 17, 2020, https://www.reuters.com/article/us-china-pacific-exclusive/exclusive-u-s-warns-pacific-islands-about-chinese-bid-for-undersea-cable-project-sources-idUSKBN28R0L2.

60 Bruce Schneier writes that "For years, the US and the Five Eyes have had a monopoly on spying on the Internet around the globe. Other countries want in. As I have repeatedly said, we need to decide if we are going to build our future Internet systems for security or surveillance." Bruce Schneier, "China Spying on Undersea Internet Cables," schneier.com, April 15, 2019, https://www.schneier.com/blog/archives/2019/04/china_spying_on.html.

61 Cheng Qingqing, "Huawei's undersea cable project moves forward in SE Asia," *Global Times*, June 20, 2019, https://www.globaltimes.cn/content/1155060.shtml.

62 Danielle Kehl, Kevin Bankston, Robyn Greene, and Robert Morgus, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity, New America*, 16, July 2014, https://static.newamerica.org/attachments/534-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/Surveilance_Costs_Final.pdf.

2020.[63] Private companies with control of Internet infrastructure already help states conduct espionage, and that risk is pronounced when the entity in question is not privately owned but state-controlled. This is doubly the case in a country like China, where authoritarian surveillance practices—not fully comparable to surveillance carried out in the United States—mean there is an even greater likelihood that Beijing would use this vector of influence over the undersea cable infrastructure if desired.

Recommendation Previews

Companies have long led the development of the Internet globally, especially in the United States and many other liberal democracies. In kind, it has been and generally remains a positive and necessary component of submarine cable construction that many firms from many countries collaborate to fund these financially expensive and logistically intensive projects. But growing exertion of authoritarian control over Internet companies, especially from Beijing and Moscow, calls into question the independence of some of the firms in these consortia, and thus increases cybersecurity and resilience risks. Key policy issues include:

- **Oversight:** Federal inspection and monitoring of foreign telecoms operating in the United States is essential for identifying vectors of potential authoritarian influence on Internet security and resilience. Yet the US government body responsible for monitoring foreign-owned telecoms in the United States for security risks is not adequately resourced to monitor the full spectrum of security and resilience risks posed by certain foreign telecoms. In response, the US Congress should statutorily authorize the executive branch committee responsible for these reviews, ensuring it has the resources and authorities it needs to screen foreign cable ownership structures for national security risks (Recommendation 1).

- **Transparency:** TeleGeography's Submarine Cable Map data is comprehensive, but it is also limited by its use of public sources. The coding of cable ownership for this report—specifying if firms are privately owned, state-controlled, or have an unclear ownership structure (just five out of the 383 cable owners)—was similarly dependent upon open sources and, therefore, has many limitations. Limited transparency into submarine cable ownership structures limits the ability of third parties (researchers, third-party firms, etc.) to evaluate the risks of a government exerting control over that infrastructure in ways that compromise its security and/or resilience. Increased authorities and resources for the US committee that screens foreign telecoms for security risks would help to address this problem (Recommendation 1). The State Department should also conduct a study on ways to better integrate undersea cables in cyber capacity-building and foreign assistance programs for infrastructure, focused on these security and resilience questions (Recommendation 5).

63 Renato Mota, "Submarine cable that will connect Brazil and Europe is anchored in Fortaleza," Olhar Digital, December 14, 2020, https://olhardigital.com.br/en/2020/12/14/noticias/cabo-submarino-brasil-europa-ancorado-fortaleza/.

Trend 2: Companies Using Remote Management Systems for Cable Networks

In addition to who owns and builds undersea cables, the technologies used to manage them increasingly create risks to cable security and resilience. More companies are using remote management systems for submarine cable networks—tools to remotely monitor and control cable systems over the Internet—which are cost-compelling because they virtualize and possibly automate the monitoring of cable functionality. Yet when these cable management tools are connected to the global Internet, they expose undersea cables to new risks of hacking—both for monitoring cable traffic and disrupting it altogether. This second key trend presents a more operational risk to Internet security and resilience than the previous trend; much of the opportunity and responsibility for the US government to renew its engagement with allies, partners, and companies to protect these management systems comes back to practices like software updates and security standards. But this risk is still entangled with the other two trends: because companies are increasingly using remote network management systems, states have incentives to hack into them to monitor traffic; and because the volume and sensitivity of traffic sent on the global Internet is increasing, intercepting or disrupting that data is more attractive to governments and criminal actors—and easier through these poorly secured and Internet-connected technologies.

The US Office of the Director of National Intelligence (ODNI) classifies the possibility of cyberattacks against cable landing stations as a "high risk" to national security.[64] In a worst-case scenario,[65] hackers could breach multiple remote network management systems used to control different submarine cables to completely disrupt the flow of Internet data across that infrastructure. This could be targeted at the US mainland or at another geographic area of interest to a malicious actor (e.g., a conflict zone) to either greatly slow or corrupt Internet traffic delivery and/or force Internet traffic intended for that region to be routed through other points on the global Internet network. Once in control of cable companies' remote management systems, these attackers could wreak this kind of havoc on Internet traffic flows from their keyboards, miles away.

Adversaries, for instance, could execute such a targeted attack during a military conflict or other geopolitical crisis to intercept or disrupt large volumes of Internet traffic; terrorist organizations with requisite offensive cyber capabilities, to give another example, could even more destructively attempt to slow swaths of Internet traffic headed to the United States or another country, perhaps timed with some kind of kinetic attack. Potential compromise of cable management systems was a concern at least a decade ago, when Nokia introduced submarine cable terminal equipment: it had failed to clearly show the systems were not vulnerable to the attacks used in the Stuxnet operation against Iran.[66] But the planned expansion of Internet-connected remote network management systems today has made this security problem dramatically worse for the United States, the US private sector, and US allies and partners around the world.

Every submarine cable must have at least two landing points—spots at which it reaches a country's shoreline and where its fiber-optic signals are transmitted to users over land. Landing stations play a key part in the operation of undersea cables. They can perform many functions, including terminating international cables, supplying power to cables, and acting as a point of domestic and/or international connection.[67] Their physical security is also important, as natural disasters and intentional damage can stop the cables from transmitting Internet data.[68] Historically, the operating centers located at or near these landing points have been largely managed by on-site personnel or through tools that are not directly connected to the Internet.[69] These systems

64 U.S. Office of the Director of National Intelligence, *Threats to Undersea Cable Communications*, 7, September 2017, https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf.

65 This is the author's own scenario as opposed to one described by the ODNI.

66 U.S. Office of the Director of National Intelligence, *Threats to Undersea Cable Communications*, 14.

67 United Nations International Telecommunication Union, "Cable Landing Stations: Building, Structuring, Negotiating and Risk," 2, 2017, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Submarine%20Cable/submarine-cables-for-Pacific-Islands-Countries/Cable%20Landing%20Stations%20SNCC.pdf.

68 For example, see a list of security and disaster mitigation infrastructure typical to a landing station: Samia Bahsoun, "Part I: Undersea Cable System: Technical Overview & Cost Considerations," NANOG, 6, June 2008, https://archive.nanog.org/meetings/nanog43/presentations/Demystifying_Bahsoun_N43.pdf.

69 Remote control mechanisms were still used, however. For example, see: Mitsubishi Electric, "Optical Submarine Cable Systems: MF-1280GWS (DRY PLANT)," May 29, 2008, http://www.mitsubishielectric.com/bu/communication/transmission/submarine/products/dryplant_b.html; United Nations International Telecommunications Union. ITU-T Recommendation G.977. *Series G: Transmission Systems and Media, Digital Systems and Networks*, 25, Geneva: International Telecommunications Union, December 2006. 25, https://www.itu.int/rec/T-REC-G.977-200612-S/en.

were built for tasks such as ensuring signal connectivity and maintaining power flows.[70] It is these operational tools, often managed by private firms, that help enable the geopolitically consequential activities on the global Internet, from personal communications to financial transactions, scientific research, and the sending of government documents, for which data is hauled over cables.

Now, however, more companies that manage submarine cables are connecting their landing points and operating centers to remotely controllable "network management systems." These tools are compelling to companies because they do not require personnel to be on site. Working from afar, companies can monitor the data sent over cables and even alter fiber-optic signals, all through a virtual interface. Yet it is not just about cost and convenience. Optical fiber technology in undersea cables has grown more sophisticated over the last two decades. Thus, managing a cable system and a landing station now includes managing complex signal configurations.[71] Hence the demand for more sophisticated cable management software that is Internet-connected and can exert physical changes to fiber signals themselves.

This push for cost-effectiveness and remote monitoring introduces new vectors of cybersecurity risk. By introducing a software-driven, "virtualized" layer of control over cable systems—one connected to the Internet—cable owners are exposing themselves to potential hacks of submarine cables through that technology. These hacks could disrupt or degrade signals traversing the submarine cable fibers. For instance, TE Subcom, a US-incorporated firm that builds cable equipment, offers an "Ocean Control suite" that uses application programming interfaces (APIs) to offer "extensive remote programmability and control of an entire communications network, both terrestrial and undersea."[72] Malicious control of those systems could enable actors to harmfully alter or disrupt Internet traffic delivery across key cables.

The risk of cable disruption through hacking is magnified by poor security practices by some of these software vendors (e.g., poorly securing communications between the virtualization interface and the physical infrastructure).[73] The relative lack of diversity among remote management system vendors creates additional security risk through centralization[74]—compromises of one technology (e.g., backdooring updates, discovering a new vulnerability, etc.) could have wider effects on cables. Many remote network management systems also use common operating systems like Linux or Microsoft Windows with which more malicious actors are likely familiar, as opposed to highly specialized and obscure interfaces that are sometimes used in such infrastructure control systems.[75] And the way vendors update and can control systems once deployed on the customer end might introduce other kinds of risks into this part of the cable supply chain. Malicious actors could exploit these realities to disrupt cable signals.

Beyond disruption, hacks of remote network management systems could enable malicious actors to intercept data flowing through landing stations. Hacking into poorly secured network management systems to intercept and collect traffic can be relatively low-cost.[76] Governments already turn to private companies within their borders to collect data for a range of purposes, including legitimate foreign intelligence and law enforcement purposes and/or unchecked surveillance, depending on the specific country and specific case.[77] In many democracies, this can create tensions with private companies that want to limit their involvement with state espionage activities and/or have other obligations such as privacy, transparency,

70 Nomura Kenichi and Takeda Takaaki, "Optical Submarine Cable Network Monitoring Equipment," *NEC Technical Journal* 5 (1) (2010): 33, 33-37, https://www.nec.com/en/global/techrep/journal/g10/n01/pdf/100108.pdf.

71 Ibid.

72 LightWaveOnline.com, "TE SubCom launches Ocean Control suite for remote programmability and terrestrial and undersea cable network control," May 10, 2018, https://www.lightwaveonline.com/network-design/article/16676184/te-subcom-launches-ocean-control-suite-for-remote-programmability-and-terrestrial-and-undersea-cable-network-control; TE SubCom, TE SubCom announces Ocean Control suite, first offering of full network programmability for undersea domain, press release, May 8, 2018, https://www.subcom.com/documents/Ocean_Control_Full_Network_Programmability_TE_SubCom_8MAY2018.pdf.

73 Michael Sechrist, *New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems*, Harvard Belfer Center for Science and International Affairs, 10, 12-15, February 2012, https://www.belfercenter.org/sites/default/files/files/publication/sechrist-dp-2012-03-march-5-2012-final.pdf.

74 Daniel Voelsen, *Cracks in the Internet's Foundation: The Future of the Internet's Infrastructure and Global Internet Governance*, German Institute for International and Security Affairs, 21, SWP Research Paper 14, November 2019, https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2019RP14_job_Web.pdf.

75 Sechrist, *New Threats, Old Technology*, 13; Kenichi and Takaaki, "Optical Submarine," 35.

76 DJ Pangburn, "Wiretapping Undersea Fiber Optics Is Easy: It's Just a Matter of Money," *VICE*, July 22, 2013, https://www.vice.com/en/article/wnnmv9/undersea-cable-surveillance-is-easy-its-just-a-matter-of-money.

77 The US government itself is no stranger to turning to private companies for foreign intelligence collection. See, for example, Craig Timberg and Ellen Nakashima, "Agreements with private companies protect U.S. access to cables' data for surveillance," *Washington Post*, July 6, 2013, https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html.

Physical Threats to Landing Stations

Physically securing cable landing stations against power outages, natural disasters, and malicious activity (e.g., manual insertion of monitoring equipment) remains a key part of protecting undersea cables. This is particularly the case in a nation-state context where intelligence services could work to compromise landing stations through human operatives, such as planting monitoring equipment directly onto landing station infrastructure. Much national security concern around potential physical disruptions to submarine cable infrastructure has focused on terrorism risks, where attackers could seize or physically destroy landing station infrastructure. The focus in this section remains on remote hacks of network management systems because of the accelerating nature of the risk, but investments in physical security and continuity-of-operation protocols for cable landing stations remain critically important for the private sector as well.

and customer protections.[78] All to say, there may already be technical mechanisms in place for private companies to intercept data for governments, and third parties could potentially abuse those mechanisms. Governments can also hack directly into cable management systems to steal data.[79] Yet securing undersea cable management systems against malicious data theft and monitoring is even more challenging when (a) more companies' remote management tools are Internet-connected and (b) many cables and their operations centers are controlled by consortia of firms.[80] As the data compiled for this report show, these owners may be spread across many countries and are in some cases state-controlled. It is an important challenge for Internet security and resilience, as protecting the Internet data itself also means protecting the infrastructure across which they travel.[81]

In sum, network management systems deployed by cable owners increase submarine cables' attack surface: with remote, Internet-connected control systems linked directly to the Internet's physical infrastructure, hacks can be conducted from afar and "could physically change a network or drop communication paths altogether."[82] Attackers need not be physically on site to undermine Internet security and resilience. Developers of these management systems may also not prioritize securing them due to poor market incentives; like many industrial control systems, these technologies are most often designed for convenience and functionality above cybersecurity. Further, restoring these systems once compromised may not be a straightforward effort: "legal, cultural, and language barriers may limit the ease and effectiveness of information flow in the event of a disruption, and depending on where cable disruption symptoms appear, public agencies without a local presence may struggle to coordinate a timely response."[83] It is an exceptionally impactful case in the broader Internet infrastructure security conversation. All of this presents risks to the security and resilience of the Internet.

Recommendation Previews

The US government has few measures in place to ensure the software control systems for key traffic hubs, even those located in the United States, are secure; companies may be deploying poorly secured remote network management systems that potentially compromise the security and resilience of US Internet connectivity and Internet data. The US private sector also co-owns only a portion of global undersea cables, often with other companies. That said, the US government has valuable nexus over submarine cables given what influence the US private sector does have over cables (discussed more in the next section) as well as the private sector's control of undersea cables touching US borders. Taken together, this gives the US government an opportunity and responsibility to expand cooperation with allies, partners, and the US private sector to build solutions to the operational security risks of remote cable management systems. This could produce

78 Susannah Larson, "Submarine Cable Network Security Panel," PTC '17 Submarine Cable Workshop, 6, January 15, 2017, https://online.ptc.org/assets/uploads/papers/ptc17/PTC17_SUN_WS_Subcable%202_Stafford.pdf.

79 See, for example, Lana Lam, "EXCLUSIVE: US hacked Pacnet, Asia Pacific fibre-optic network operator, in 2009," *South China Morning Post*, June 22, 2013, https://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator.

80 Panagiota Bosdogianni, "Submarine Cable Network Security Panel," PTC '17 Submarine Cable Workshop, 8, January 15, 2017, https://online.ptc.org/assets/uploads/papers/ptc17/PTC17_SUN_WS_Subcable%202_Stafford.pdf.

81 NATO Cooperative Cyber Defence Centre of Excellence, *Strategic importance of, and dependence on, undersea cables*, 3, November 2019, https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.

82 Ibid., 14.

83 Ibid., 13.

valuable effects on scaling up security across the Internet ecosystem. Key policy issues include:

- **Security Baselines:** Remote network management systems, as with many industrial control systems, are often poorly secured. Cable owners using these technologies are exposing the physical infrastructure itself to possible surreptitious monitoring or outright disruption. In response, the US government should use the point of leverage it has available—incentivizing private firms incorporated in the United States to use more secure remote network management systems for undersea cables, founded on a set of clear cybersecurity baselines and best practices (Recommendation 3). While the order is more focused on information technology, this aligns in principle with the Biden administration's executive order that places priority on addressing the security of "critical software" in the supply chain.[84] Amazon, Facebook, Google, and Microsoft, increasingly responsible for cable construction worldwide (discussed more in the third section), should craft and publish strategies for promoting the security and resilience of their cable infrastructure in response to these risks (Recommendation 8).

- **Threat Sharing:** The submarine cable industry, despite these growing digital threats, still does not have robust mechanisms in place to share threat intelligence on undersea cable hacking risks. Cable systems are, meanwhile, only more attractive hacking targets as they become more important for key societal functions—from civilian communication and public health to government document sharing and scientific research—and as the data across them becomes more sensitive (discussed more in the next section). In response, US-based submarine cable owners should work with federal, state, and local authorities to establish public-private Information Sharing and Analysis Centers (ISACs) for cyber threats to undersea cables (Recommendation 7).

84 White House, Executive Order on Improving the Nation's Cybersecurity, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Trend 3: Increasing Volume and Sensitivity of Data Sent Over Undersea Cables

There is more data sent over undersea cables each day, and that data is also becoming more sensitive. The COVID-19 pandemic has accelerated the former trend, shifting more living, learning, and working online and dramatically increasing the amount of traffic moving over the Internet's physical backbone.[85] 5G will similarly contribute to a massive increase in Internet data routed over cables. The latter trend, increasing data sensitivity, is predominantly tied with the rise of cloud computing—where private companies rent out storage space and processing power to clients—as these companies are increasingly moving previously offline or back-end functions and data onto the global Internet. The effect on economic and national security is straightforward: the more data, and the more sensitive data, that travels over undersea cables, the more important their security and resilience becomes. Errors with and disruptions to this traffic become more disruptive to society as a whole, harming individuals as well as public and private organizations across health, commerce, defense, and transportation and logistics. States exerting more control over cable owners know that the growing volume and increasing sensitivity of Internet data makes data interception and manipulation more valuable. Those looking to hack into cable landing stations or remote cable management systems likewise recognize the growing value of this sensitive data.

There are many metrics that capture the growing volume of data sent over undersea cables: Hundreds of millions of tweets and billions of emails and other messages are sent online daily.[86] In 2020, Internet users worldwide spent an average, per capita, of three hours online every day, and that is expected to rise by 6 percent in 2021.[87] More American households are subscribed to the Internet every year.[88] One estimate says global interconnection bandwidth will grow at a 45 percent compound annual growth rate from 2019 to 2023,[89] yielding a potentially massive increase in the volume of data hauled by submarine cables in just the next few years.

Although much discussion of 5G infrastructure focuses on the network's software-driven nature, 5G does not eliminate the need for undersea cables—on the contrary, 5G will only further increase the volume of data flowing over cables. For Internet content to be sent over cellular networks today, that cell tower network must connect to servers and cables that can deliver the endpoint-housed data (like for smartphone users browsing TikTok or logging into a mobile banking app). In other words, because Internet content itself is not stored on cell company networks, once a phone makes a request for Internet data, the cellular tower infrastructure must at some point connect to the global Internet to retrieve it. This will not change with 5G. The fifth generation of cellular network technology may use less hardware and have more sophisticated software functionality than its 4G predecessor. But if 5G networks are going to deliver the data speed and bandwidth that experts predict, they will rely on fast and resilient submarine cable infrastructure to carry the Internet content ultimately delivered to 5G network users.[90] In turn, 5G's higher data speed and bandwidth, and constant communication with high volumes of Internet of Things (IoT) devices, will result in even more data flowing over submarine cables.

Simultaneously, data sent over submarine cables is increasingly sensitive to the US economy and national security, and this second shift is tied to the accelerated growth of cloud computing. US cloud service providers are routing more data over the Internet as their customer bases grow. Many critical sectors are becoming more dependent on cloud computing by the month, including firms in financial services, energy, healthcare, shipping and logistics, and defense that pay cloud service providers to store and send their data. In practice, this means that more of their information is being sent across the global Internet instead of just back-end, intranet systems.[91] It is in many cases highly sensitive, and highly valuable, data. Financial service providers might store customer data in the cloud for real-time access; transportation and logistics companies may run their inventory management systems on a third-party cloud system.

85 TeleGeography, "State of the Network: Updates on COVID-19," accessed January 14, 2021, https://www2.telegeography.com/network-impact.

86 Jeff Desjardins, "How much data is generated each day?" World Economic Forum, April 17, 2019, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

87 Statista, "Average daily time spent per capita with the internet worldwide from 2011 to 2021," accessed January 14, 2021, https://www.statista.com/statistics/1009455/daily-time-per-capita-internet-worldwide/.

88 *Internet usage in the United States* (New York: Statista, 2020).

89 Olu Rowaiye, "North America to Consume 41% of the World's Interconnection Bandwidth," Equinix, October 14, 2020, https://blog.equinix.com/blog/2020/10/14/north-america-to-consume-41-of-the-worlds-interconnection-bandwidth/.

90 See, for example, Brian Lavallée, "5G wireless needs fiber, and lots of it," Ciena, July 11, 2019, https://www.ciena.com/insights/articles/5G-wireless-needs-fiber-and-lots-of-it_prx.html.

91 Justin Sherman and Tinajiu Zuo, *Cloud Computing As Critical Infrastructure, Atlantic Council*, forthcoming.

Defense and intelligence contractors may also run national security-critical services on government-approved cloud systems to offload the costs of managing servers in-house. Government agencies are moving to the cloud at varying speeds and to varying degrees; not every implementation involves an equal dependence, at present, on third-party cloud systems housing sensitive data and services. But cloud adoption by the defense base is growing. Every time companies in these sectors retrieve sensitive data and services from the cloud, that information is potentially routed over submarine cables, especially when data transfers are intercontinental (e.g., a company linking to a cloud server overseas). Compromising this data could enable criminals, terrorists, and especially foreign nation-states to use it for their own gain. The sensitivity of the data sent over the global Internet is also shifting alongside its rapidly growing volume.

The accelerated growth of cloud computing is directly relevant to how the US government can better work with allies, partners, and companies to protect submarine cables. This is because these providers are not just moving more data over Internet infrastructure—they increasingly own that infrastructure too, giving them a growing responsibility to protect its security and resilience. As the Submarine Telecoms Forum's 2020 industry report put it, "providers such as Amazon, Facebook, Google and Microsoft are completely transforming the submarine cable market. They are no longer reliant on Tier 1 network operators to provide capacity and are simply build(ing) the necessary infrastructure themselves."[92] This accelerated investment became clear in 2019, when TeleGeography noted that Facebook as well as Amazon, Google, and Microsoft—the three major US cloud providers—were taking a newly active role in the changing shape of the Internet.[93]

The US private sector already has a notable influence on submarine cables. Figure 8 shows the number of undersea cables deployed worldwide with at least one private US owner.

US government cooperation with allies and partners abroad, as well as with the US private sector, is essential to better securing this vital Internet infrastructure. One hundred and six of the 475 undersea cables (22 percent) deployed worldwide as of December 2020 have at least one US private sector owner. The US government itself only has ownership in two cables, which are linked to Guantanamo Bay.[94] This means the US private sector has a notable influence on the global Internet's physical shape, considering the US has at least one corporate owner with stake in 22 percent of the world's undersea cables. By extension, the US private sector also has a notable influence on the security and resilience of the data sent across that infrastructure. At the same time, however, it is not a dominant influence. Many cables with US ownership have several other corporate owners from other countries. Over two-thirds of cables do not even have a US-incorporated owner. Sensitive data for critical US sectors, from public health to financial services, is routed not just over American-owned infrastructure but over that owned by many firms around the world.

US cloud providers are a unique point of leverage for the US government as they increasingly invest in undersea cables. Unlike in China or Russia, however, where state leverage over Internet companies is used for the likes of BGP traffic hijacking, the US government can use this nexus to incentivize better security. This is because the US "hyper-scalers" Amazon, Google, and Microsoft—nicknamed as such for their scaled-up infrastructure—have been spending substantially more money on submarine cables in recent years. (They also dominate the cloud computing market, a centralization which itself presents economic and security risks.[95]) Their American incorporation and substantial federal contracting present an opportunity for the US government to incentivize better protections on their cable systems. In tandem, these cloud providers' responsibility to protect the infrastructure's security and resilience grows. Figure 9 illustrates this growing cloud provider investment.

The three "hyper-scalers" investing more money in submarine cable development does not by itself mean more cloud data is sent across the cables—owning an undersea cable is different than relying on it to carry data. However, given that the amount of Internet bandwidth consumed by cloud service providers *is* growing, the corresponding increase in hyper-scaler investment in submarine cables appears to reflect these firms' strategic interest in resilient physical infrastructure that hauls data quickly. Maintaining a secure and resilient submarine cable network is critical to safely and reliably routing cloud service provider data. Maintaining cable ownership is also an opportunity for these firms to profit off growing Internet traffic demands worldwide in the process.[96] Not all cloud data is routed over undersea cables, but it becomes more likely as the global

92 Submarine Telecoms Forum, Inc., *Submarine Telecoms Industry Report: 2020/2021 Edition*, October 23, 2020, https://subtelforum.com/products/submarine-telecoms-industry-report/.

93 Jayne Miller, "This is What Our 2019 Submarine Cable Map Shows Us About Content Provider Cables," *TeleGeography Blog*, March 19, 2019, https://blog.telegeography.com/this-is-what-our-2019-submarine-cable-map-shows-us-about-content-provider-cables.

94 These are the GTMO-1 (ready for service in 2016) and GTMO-PR (ready for service in April 2021) cables.

95 Sherman and Zuo, *Cloud Computing*.

96 Amazon Web Services, for example, touts its global Internet infrastructure backbone on its website: AWS.Amazon.com, "Global Network," accessed January 14, 2021, https://aws.amazon.com/about-aws/global-infrastructure/global_network/.

cloud infrastructure expands (with many servers around the world) and many cloud service provider clients have operations based in multiple countries (and thus require Internet data to be hauled intercontinentally).

Google is by far the most active investor in undersea cables, with ownership stake in ten different cables that should be ready for service in 2021. It remains to be seen how many more cables Google might invest in for 2022. It is unlikely these investments are going to subside, based on estimates that place global spending on cloud services at hundreds of billions of US dollars a year and rapidly growing.[97] Digital services depend on underlying physical infrastructure, so rising dependence on the former means rising dependence on the latter. This is also one explanation for why Facebook, which does not offer cloud services but runs its own Internet platform, is investing more in cable ownership.

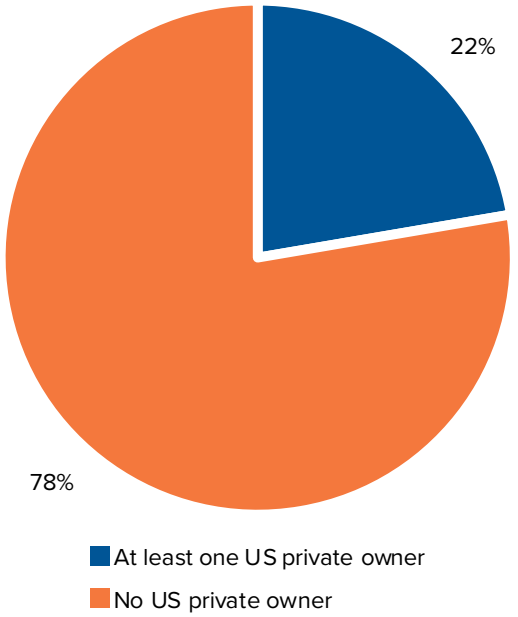
Facebook's investment in submarine cable development is, notably, even more accelerated than that of Amazon or Microsoft. Amazon currently has ownership stake in a 2020 cable and a 2022 cable, and Microsoft has ownership stake in just two 2021 cables, while Facebook has ownership stake in three cables deployed in 2020 alone. The firm has made a concerted push to expand physical Internet infrastructure around the world, including as a way of growing its market power.[98] Submarine cable investments are, therefore, attractive not just to cloud service providers but to other private Internet companies that need fast and reliable data routing infrastructure. All the while, the more these companies invest in shaping the physical topology of the Internet and maintaining cable networks, the greater their responsibility to protect its security and resilience. They are the ones with direct ownership stake in the infrastructure. They may also control many of the data centers to and from which significant volumes of Internet data flow. Further, there are many benefits to having independence between private US cable owners and the US government compared to other countries where the state is heavily involved in the building and management of most Internet infrastructure—and there is a benefit to keeping it that way. But that means these private firms must do more to address security and resilience risks.

Recommendation Previews

Undersea cables underpin global Internet traffic delivery, routing data every day for financial transactions, scientific research, government communications, personal messaging, and more. There is not just a growing volume of data traversing undersea cables, however; the sensitivity of that data is also increasing. Explosive growth in cloud computing has led more critical sectors, from defense to health to finance to supply and logistics, to transition their data and services to the cloud. In the process, more and more sensitive information, vital to everything from global financial markets to public health, is transmitted over undersea cables. This makes securing the cables, and ensuring their resilience, an urgent issue for the US government in cooperation with allies, partners, and the private sector. The growing centralization of new, US-connected cable infrastructure in the hands of a few cloud service providers (Amazon, Google, and Microsoft) as well as Facebook increases the urgency of ensuring proper investment in security and resilience. Key policy issues include:

- **Fast Repairs:** The increasing volume and sensitivity of data routed over submarine cables means security compromises and service disruptions can inflict even greater harm on economic and national security.

Figure 8: Cables with at Least One Private US Owner (December 2020 Snapshot)

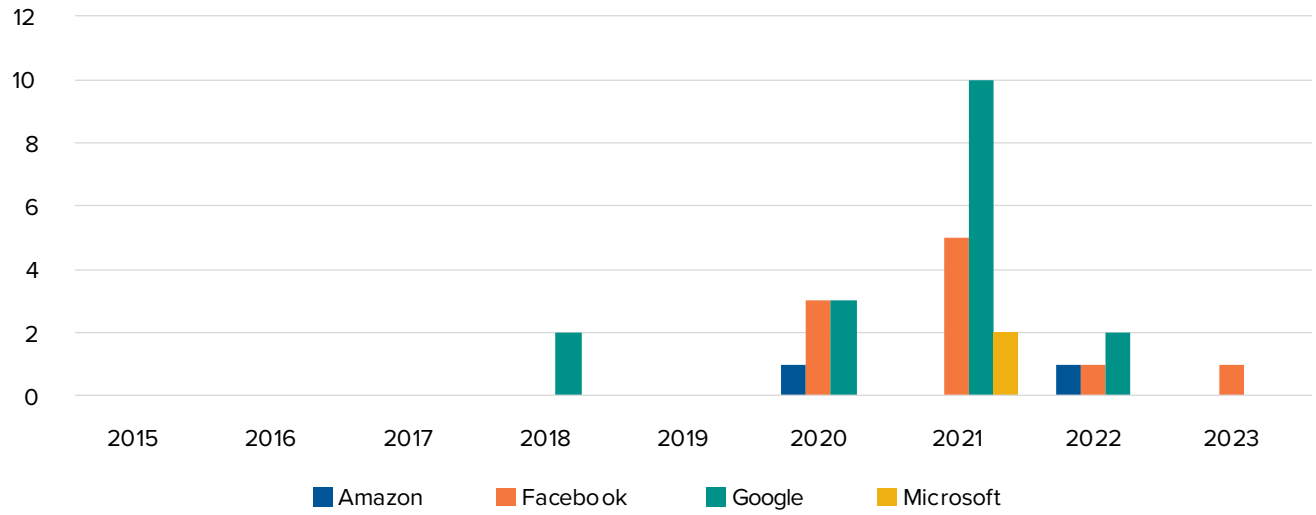


Source: Data from TeleGeography's Submarine Cable Map website visualized by author.

97 Statista, "Public cloud services annual growth rate worldwide from 2020 to 2022, by segment," accessed January 15, 2021, https://www.statista.com/statistics/258718/market-growth-forecast-of-public-it-cloud-services-worldwide/; Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021, press release, November 17, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021; Kimberly Mlitz, "Cloud Computing – Statistics & Facts," Statista, March 30, 2021, https://www.statista.com/topics/1695/cloud-computing/.

98 For example, see a Facebook blog post touting the company's investment in undersea Internet cables: Najam Ahmad and Kevin Salvadori, "Building a transformative subsea cable to better connect Africa," Facebook Engineering, May 13, 2020, https://engineering.fb.com/2020/05/13/connectivity/2africa/.

Figure 9: Current Big Tech Cable Ownership, by Year Ready for Service (December 2020 Snapshot)



Source: Data from TeleGeography's Submarine Cable Map website visualized by author.
Note: Cables listed in the future are coded based on their expected ready-for-service date.

Coordinating the quick repair of these cables is often difficult for private companies working with consortia of other cable owners incorporated in a range of countries.[99] The US Congress already funded the Cable Ship Security Program to speed up repairing damage to US national security-relevant submarine cables. The program is being stood up now, but at least one year into its launch, Congress should conduct a review of whether the program requires further funding (Recommendation 2). Internationally, the Department of State should conduct a study on ways to better integrate fast cable repair into capacity-building and foreign assistance work globally (Recommendation 6). And US cable owners—including Amazon, Facebook, Google, and Microsoft—should publish strategies to promote the security and resilience of their cable infrastructure, including plans on cable repairs (Recommendation 8).

- **Outage Reporting:** Cable outages occur for many reasons, most often not malicious: weather events, ship collisions, and other incidents can physically damage cables; power outages and other electrical or digital problems can likewise disrupt cable operations. The FCC focused additional resources on monitoring such events in 2016, but there is still more work to be done to ensure that cable outages are communicated—and responses are coordinated—in the most efficient and effective ways possible. The FCC should focus more resources on interagency coordination on cable outages, as the range of data traversing submarine cables is of concern to many agencies across the federal government (Recommendation 4). This feeds into supporting other objectives, such as fast repairs of cables via the US Cable Ship Security Program mentioned above.

- **Norms:** Undersea cables are already vulnerable to espionage and cyberattack, and this is especially true with poorly secured and Internet-connected remote cable management tools. If badly secured, these systems are more susceptible to compromise and with even less advanced capabilities. In response, the Department of State should strengthen international norms against nation-states damaging or disrupting undersea cables (Recommendation 5). Because of the legal complexity of protecting international cables located outside of a country's territory, the frequently multiparty ownership structures of undersea cables, and other factors, "international State involvement is critical to the twin goals of victim compensation and deterrence against future depredations."[100] Especially when it comes to authoritarian governments in Beijing and Moscow, and Internet governance "swing states" who may find the idea of cable damage or disruption compelling, the US government must act in concert with allies and partners to bolster norms against those actions.

99 There are a number of procedures available to firms to share information about cable outages and repairs with other implicated companies. See, for example, International Cable Protection Committee, "Recommended Co-ordination Procedures for Repair Operations near Active Cable Systems," ICPC Recommendation No. 4, Issue: 8C, February 24, 2014.

100 Mick P. Green and Douglas R. Burnett, *Security of International Submarine Cable Infrastructure: Time to Rethink?* International Cable Protection Committee, 8, 2008.

Recommendations

For all the attention paid to communications technologies like satellites or 5G cellular networks, the vast majority of global Internet communications still travel through metal-encased, fiber-optic tubes laid along the ocean floor. It is these submarine cables, deployed in the hundreds globally, that help haul everything from scientific research to e-commerce to government communications around the world. The international delivery of Internet data depends directly on this infrastructure's function. Much of this infrastructure is multi-owned by consortia of private and state-controlled firms. And, importantly, this physical infrastructure is not set in stone. Just as the Internet was created and built by humans, the Internet's physical shape continues to be shaped by humans, as cable owners look to expand global Internet connectivity and upgrade older physical infrastructure. As societal reliance on the Internet grows, more investments in submarine cables reflect a concurrently growing need to ensure the Internet's physical backbone is secure and resilient.

Three trends, however, are accelerating risks to the security and resilience of undersea cables. First, authoritarian states are reshaping the Internet's physical topology and digital behavior through companies, introducing new possibilities of espionage and disruption, and reshaping the Internet infrastructure to favor their Internet governance models. Second, more cable owners are linking cable landing stations to remote network management tools, which exposes cables to hacking and disruption. And third, the volume of Internet data sent daily grows, as does its sensitivity; thus, society is more reliant on cables being secure and resilient, and there are more incentives for states and other actors to intercept, disrupt, or manipulate the delivery of this valuable information.

But even with the influence the US private sector has on global cable development, the private sector cannot go it alone. Poor market incentives for robust security—combined with new threats and an internationally collaborative system of cable construction and management—mean the US government must also better engage with allies and partners to protect the security and resilience of this submarine cable infrastructure. To this end, this report makes the following recommendations for the US government, along with the private sector and allies and partners, to better protect the security and resilience of submarine cables:

1. **The US Congress** should statutorily authorize the US executive branch body responsible for monitoring foreign-owned telecoms in the United States for security risks: the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (formerly the informal Team Telecom).[101] This would provide it with the necessary funding, review authority, and formal structure to better screen foreign telecoms that own cables. The newly renamed organization is a coordinating entity between several federal agencies, with the FCC playing a key role on the telecom referral and licensing side, and the Department of Homeland Security (DHS) and the DOJ playing a key role on the security review side. However, a June 2020 Senate report, produced after months of investigations into the organization, found the committee had been conducting "minimal oversight" of Chinese state-owned telecoms in the United States in ways that "undermined the safety of American communications and endangered our national security."[102] Resource constraints were compelling the participating agencies to devote more time, money, and personnel to interagency work on the Committee on Foreign Investment in the United States (CFIUS) than the telecom security review committee.[103] Because it did not have formal authorities and structure, the group also "had no formal, written processes for reviewing applications or monitoring compliance with security agreements," and if it did not choose to enter into a security agreement with a foreign carrier, it lacked other means of getting insight into the carrier's operations.[104] The US Congress should mitigate this problem by statutorily authorizing the executive branch committee, just as it did in 2007 with CFIUS, to give the organization more resources and authorities to more expansively screen foreign cable ownership for national security risks. If the US government wants to be more proactive in assessing the national security and resilience risks to the

101 Team Telecom, a previously ad hoc group, was transformed into an official executive branch committee as a result of a 2020 executive order. See, Trump White House, "Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," April 4, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-establishing-committee-assessment-foreign-participation-united-states-telecommunications-services-sector/.

102 United States Senate Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, 2, June 2020, https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.

103 Ibid., 43-44.

104 Ibid., 3-4.

Internet's physical backbone, it must invest more time and resources into conducting those reviews, and it must give more authorities to the committee to do so, including legally requiring a periodic reassessment of foreign carriers and allowing the organization to inspect foreign carriers with which it has no existing security agreement.[105] This expanded review process should include a more intensive focus on ownership structures of cable owners and cable consortia, as more authoritarian governments work to reshape the Internet's physical topology and digital behavior through sometimes opaque ownership structures and influence. It should also include considering the security risks of remote network management systems deployed by cable owners. And the expanded security review process should consider not just the direct owner of a particular cable but all of the providers and subsidiary firms that interact with the cable or its data en route.

2. **The US Congress** should conduct a study, starting no earlier than one year into the program's launch, on the Cable Ship Security Program that was authorized in the National Defense Authorization Act (NDAA) for 2020.[106] The Department of Transportation is currently in the process of standing up the program with two vessels, so that government-authorized, privately owned ships are on standby to repair damaged submarine cables relevant to US national security.[107] This program, therefore, helps ensure that alongside commercial investment in cable resilience, the US government is taking steps to repair damaged submarine cables more quickly than they might otherwise be if left entirely up to the private sector. Far from a purely national security issue, though, the Cable Ship Security Program also promises many economic and public benefits for the United States in the way of sped-up repairs—and as such, there are many stakeholder departments and agencies across the federal government with equities in the program. The program is beginning with two vessels, but it is possible the US government may ultimately require more. Congress should, therefore, conduct a review of the Cable Ship Security Program beginning no earlier than one year into its full launch, exploring whether additional funding for more vessels would bolster submarine cable security and resilience for the United States.

3. **The US executive branch** should create and promote the use of security baselines and best practices for cable remote network management systems. More cable owners are deploying Internet-connected industrial control systems to remotely manage complex cable infrastructure. These systems could be remotely compromised to disrupt or deny the delivery of Internet data across cables, a risk compounded by the poor market incentives for developers of these technologies to legitimately prioritize cybersecurity. As such, the National Institute of Standards and Technology (NIST) should create a set of security standards and best practices for vendors that build cable remote network management systems, and for the submarine cable owners that ultimately deploy those technologies at cable landing stations. NIST's deep technical expertise and widely respected framework-creation process makes it well suited to craft a list of security standards and best practices for the private sector. Then, the US executive branch, particularly large and influential agencies like the Department of Defense, should consider adopting those security baselines and best practices into procurement requirements for any companies doing business with the federal government that also own undersea cables carrying US, and likely US government, data. If the US government is going to have more of its data routed over the global Internet via the public cloud in the coming years, it should be invested in protecting the security and resilience of the remote technologies that manage the underlying infrastructure because their compromise could have serious effects on economic and national security.

4. **The Federal Communications Commission** should invest more resources in promoting and maintaining federal interagency cooperation on resilience threats to submarine cables. While this has been an FCC effort for several years now,[108] the growing threats to undersea cable security and resilience make this internal federal coordination an even higher priority.

105 Ibid., 9-10.

106 Rob Wittman, "The greater risk to national security you've never heard of," Defense News, January 30, 2020, https://www.defensenews.com/battlefield-tech/c2-comms/2020/01/30/the-greatest-risk-to-national-security-youve-never-heard-of/. Specifically, see the 2020 National Defense Authorization Act Section 53202: "The Secretary, in consultation with the Operating Agency, shall establish a fleet of active, commercially viable, cable vessels to meet national security requirements. The fleet shall consist of privately owned, United States-documented cable vessels for which there are in effect Operating Agreements under this chapter, and shall be known as the Cable Security Fleet."

107 Notice by the Maritime Administration, "Request for Applications To Be Considered for Enrollment in the Cable Security Fleet," *Federal Register*, January 5, 2021, https://www.federalregister.gov/documents/2021/01/05/2020-29159/request-for-applications-to-be-considered-for-enrollment-in-the-cable-security-fleet.

108 Federal Communications Commission, *Improving Outage Reporting for Submarine Cables and Enhanced Submarine Cable Outage Data*, 29-30, July 12, 2016, https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0712/FCC-16-81A1.pdf.

The FCC should focus on such measures as information sharing on resilience threats and continued reassessments of the effectiveness of outage reporting requirements, which were expanded in March 2020.[109] The agency should also work with state and local authorities to integrate cable resilience best practices into permitting decisions, which would create stronger incentives for cable owners to invest in protecting cable resilience.[110] FCC action here can help identify risks, take mitigating steps as necessary, and forge better coordination mechanisms with the private sector (including through ISACs discussed below). Preventing disruptions to cable operation can support the delivery of Internet data and thus economic and national security.

5. **The Department of State** should pursue confidence-building measures to strengthen international norms against nation-states damaging or disrupting undersea cables. The political will for any kind of international legal treaty to protect submarine cables is limited: It is difficult to imagine Beijing and Moscow signing onto any agreement that would tie their own hands vis-à-vis disruptively interfering with physical cable infrastructure, whether for strategic, conflict, or domestic repression purposes. The United States could pursue such legal agreements in bilateral or limited multilateral capacities, such as within the NATO bloc, which could communicate a commitment from global, open internet countries to not disrupting submarine cables. Nonetheless, the greatest risks of nation-state-caused cable disruptions—which could undermine human rights, the free flow of information, and economic and national security—do not come from within the NATO bloc, and constraints on potential malicious behavior must focus outside the United States' closest alliances and partnerships. Confidence-building measures are thus an additional mechanism through which the United States could work to bolster norms against damaging or disrupting cables. The Department of State, and allies and partners, could place pressure on Beijing and Moscow, as well as less-discussed "swing states" in Internet governance that may be inclined to disrupt cables. This process could generally mirror the confidence-building measures used for other cyber issues: start by working with other countries to understand definitions of key terminology—for instance, what constitutes "damaging" or "tampering with" a cable, or what constitutes illegitimate government action against undersea cables (e.g., excluding non-disruptive espionage); and also establish baseline understandings of how countries view cable protection in existing agreements (e.g., whether the United Nations Group of Governmental Experts' language on critical infrastructure applies to cables). This also must include communicating the potential costs of states engaging in cable disruption.

6. **The Department of State** should also conduct a study on ways to better integrate undersea cables into cyber capacity-building and foreign assistance programs for infrastructure worldwide, focused on security and resilience questions. Disruptions of undersea cables abroad can still undermine US economic and national security by cutting or slowing Internet connectivity to other parts of the world, and even hindering data flows to the United States. These cable disruptions can also undermine human rights, the free flow of information, and economic and national security in ally and partner countries. The Department of State should, therefore, conduct a study on ways to make this issue a more integral part of its cyber capacity-building and foreign assistance work with allies and partners. Options might include working with other governments to establish cable repair programs in their own countries, working with other governments and their private sectors to understand key risks to cable resilience, and working to ensure other governments are making fast repair and resilience requirements a key part of authorizing undersea cable construction within their jurisdictions. Boosting resilience in cable infrastructure can promote a more secure and global Internet for all.

7. **US-based submarine cable owners** should work with federal, state, and local authorities to establish public-private ISACs as threats to their submarine cable infrastructure grow.[111] Industry-specific ISACs across sectors like health, energy, and finance have become integral mechanisms through which companies share cybersecurity threat information with other firms through established and confidential channels. Though many submarine cable owners are members of these and other ISACs, no ISAC exists specifically for threat sharing among submarine cable owners. Yet as more submarine cable owners deploy remote network management systems, directly connected to

109 Federal Communications Commission, "Improving Outage Reporting for Submarine Cables and Enhanced Submarine Cable Outage Data," *Federal Register*, 85 FR 15733, March 19, 2020, https://www.federalregister.gov/documents/2020/03/19/2020-03397/improving-outage-reporting-for-submarine-cables-and-enhanced-submarine-cable-outage-data.

110 See, for example, Federal Communications Commission, *Final Report – Clustering of Cables and Cable Landings*, Communications Security, Reliability, and Interoperability Council Working Group 4A, August 2016, https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG4A_Final_091416.pdf.

111 US Office of the Director of National Intelligence, *Threats to Undersea*, 9.

the Internet, to manage complex cable infrastructure, they are introducing new levels of cybersecurity risk: malicious actors could hack into these systems to disrupt cable signals. There are also many risks posed to cables that are distinct from those posed to other parts of those owners' businesses (e.g., cloud platforms, cellular networks). US-based submarine cable owners should, therefore, establish ISACs where they can share cybersecurity threat information with one another to collectively protect submarine cable security and resilience and to increase their available intelligence for making corporate cybersecurity decisions. They should work as well with federal authorities, including the FCC and DHS, particularly the Cybersecurity and Infrastructure Security Agency (CISA), as well as state and local officials, to ensure the government also has requisite threat information to make determinations about particular cables that pose unique security risks or cables whose compromise would seriously undermine US economic and national security. That said, a key issue with threat sharing is liability. CISA's liability protections for information sharing cover private firms giving information to DHS, but the federal government should consider expanded liability protections such that private companies can also share cable threat information with, at a minimum, those in the FCC, DOJ, and intelligence community that (in addition to DHS) are presently the driving force behind cable security reviews. Other factors can hinder threat sharing, such as a perceived lack of a business case for doing so, but this may be one way to help encourage it.

8. **Amazon, Facebook, Google, and Microsoft**, whose investment in submarine cables worldwide is rapidly growing, should craft and publish strategies for protecting the security and resilience of their cable infrastructure. Information historically sent on backend systems in energy, health, financial, defense, and transportation sectors is increasingly transmitted to and from the public cloud. These four US companies are also increasingly investing in building and maintaining the submarine cables which route that and other Internet data. As such, they have an elevated responsibility to protect these systems' security and resilience: they have a direct ownership stake in the infrastructure and profit from it. Their increased focus on cable security and resilience should include such measures as greater investment in securing remote network management systems, greater investment in physically securing cable landing stations, more comprehensive plans for quickly repairing and restoring cables in the event of damage or disruption, and building and maintaining robust cable threat-sharing partnerships with one another, as well as with the US government and its allies and partners.

Conclusion

Should the US government invest more in protecting undersea cables' security and resilience, the private sector's deployment of remote network management systems would have better security baked in from the get-go, making it more difficult for adversaries and other threat actors to spy on or even completely disrupt the delivery of Internet traffic. The US executive branch group responsible for screening foreign-owned cables touching the United States would have more personnel, resources, and authorities to adequately review new and existing infrastructure projects for national security risks. Authoritarian governments intent on reshaping the Internet's physical topology in their strategic favor—to route more data through their borders, enhance their surveillance capabilities and control of key Internet chokepoints, and so on—would face a more concerted effort from the US government, the US private sector, and allies and partners globally to combat efforts to increase direct state control over Internet architecture. Disruptions to or failures in cable systems, for their part, would be repaired quickly as a result of US government-supported cable repair programs for the Internet backbone touching the United States.

Alternatively, the current trajectory of undersea cable development can continue without measures to better protect cable security and resilience. Companies will continue deploying remote network management systems without robust security baked in, enabling a range of threat actors, particularly foreign intelligence services, to tap into and spy upon traffic passing through cable landing stations—and potentially even disrupt Internet signals altogether in conflict-like scenarios. The US government will continue to under-resource the organizations responsible for inspecting foreign telecom cables for national security risks, both slowing down the time it takes for those entities to clear cable projects and increasing the likelihood of overlooking cables touching the United States that pose national security risks. All the while, authoritarian regimes, particularly in Beijing and Moscow, will continue funding submarine cable development projects globally, gradually reshaping the Internet's physical topology to encourage Internet traffic to move through their own borders and through other midpoints their security agencies can intercept. And should cables be damaged or disrupted, delayed repairs will undermine Internet traffic delivery because the US government hasn't invested sufficiently, in cooperation with US industry and allies and partners globally, in quickly fixing that infrastructure and restoring the flow of Internet traffic.

As the Internet comes under unprecedented authoritarian assault, and societal dependence on the web grows in the absence of robust and ecosystem-wide cybersecurity, the US government has an opportunity and responsibility to reinforce the global Internet's positive potential by better protecting the submarine cables that underpin it. Alterations to the Internet's physical topology shape the Internet's digital behavior, and threats to the security and resilience of submarine cables likewise impact the security and resilience of the data transmitted over that infrastructure. With much of the global cable infrastructure in the hands of private and state-controlled companies, often in consortium-style arrangements, there is no one actor in charge. Yet a different future is possible, one where security and resilience are more central decision factors in the design, construction, and maintenance of undersea cables; where the US government works more proactively with industry, allies, and partners to ensure the global Internet runs reliably and securely, even in the face of failure; and where robust security for core Internet architecture is itself a compelling alternative to authoritarian visions of a state-controlled sovereign network. The US government should seize on this opportunity and embrace this responsibility.

About the Author

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, where his work focuses on the geopolitics, governance, and security of the global internet. He is also a research fellow at the Tech, Law & Security Program at American University Washington College of Law, a cyber policy fellow at the Duke Tech Policy Lab, and a contributor at *WIRED* Magazine.

Acknowledgments

The author would like to thank Trey Herr, Shane Stansbury, Samm Sacks, Andrew Grotto, Nicholas Andersen, Laura Bate, David Hoffman, Ian Ralby, Bill Woodcock, and several other reviewers who requested anonymity for their feedback on earlier versions of this report. The author would also like to thank Laura Bate, Nicholas Andersen, Ian Ralby, and several others who requested anonymity for valuable discussions about the issues. Finally, the author would like to thank Trey Herr, Simon Handler, Will Loomis, and the rest of the Atlantic Council team for their support.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
*Rafic A. Bizri
*Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
Beth Connaughty
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
Mark T. Esper
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Frank Haun
Michael V. Hayden
Amos Hochstein
Tim Holt
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Ashraf Qazi
Robert Rangel
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*
List as of July 13, 2021

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org

The University of Texas at Austin
School of Law

SUBMITTED STATEMENT OF

KEVIN FRAZIER
AI INNOVATION AND LAW FELLOW
THE UNIVERSITY OF TEXAS SCHOOL OF LAW

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY AND THE SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

HEARING ON

"SECURING GLOBAL COMMUNICATIONS: AN EXAMINATION OF FOREIGN ADVERSARY THREATS TO SUBSEA CABLE INFRASTRUCTURE"

NOVEMBER 20, 2025

A robust undersea cable system is an essential part of achieving the nation's AI aspirations and, therefore, a target of adversaries also in pursuit of AI dominance. Inadequate attention to this critical infrastructure risks jeopardizing the substantial investments being made in AI and related technologies.[1] Consider, for example, that US hyperscalers spent around $371 billion on data centers and computing resources in 2025 alone and anticipate spending more in the future.[2] As one representative of a major lab made clear, "without the connectivity [via undersea cables] that connects those data centers, what you have are really expensive warehouses."[3] A failure to adequately maintain and protect the undersea cable system may also expose the United States and its allies to significant economic, political, and technological disruptions.[4] It follows that the scale and scope of AI ambitions rises and falls with our attention and commitment to the numerous and growing threats to our undersea cable system.[5]

There is no back-up plan. If all or even a significant number of the 20 or so cables connecting Europe to North America were disrupted,[6] for example, satellites would not serve as a viable

[1] *See* Tim Stronge, *Do $10 Trillion of Financial Transactions Flow Over Submarine Cables Each Day?*, TELEGEOGRAPHY: BLOG (Apr. 6, 2023), https://blog.telegeography.com/2023-mythbusting-part-1 [https://perma.cc/QQ3K-S2XT].

[2] Martin Stansbury et al., *Can US infrastructure keep up with the AI economy?*, DELOITTE (June 24, 2025), https://www.deloitte.com/us/en/insights/industry/power-and-utilities/data-center-infrastructure-artificial-intelligence.html [https://perma.cc/Z8VV-GL7J]; Eli Tan, *Meta Raises Its Spending Forecast on A.I. to Above $70 Billion*, N.Y TIMES (Oct. 29, 2025), https://www.nytimes.com/2025/10/29/technology/meta-spending-ai.html [https://perma.cc/T8M6-W2FA].

[3] *See, e.g.,* Magdalena Petrova, *Underwater cables are a vital piece of the AI buildout and internet — investment is booming*, CNBC (Nov. 8, 2025), https://www.cnbc.com/2025/11/08/big-tech-ai-underwater-cables.html [https://perma.cc/Z2XE-G2PP] (quoting Alex Aime, vice president of network investments at Meta).

[4] *See* JOCELINN KANG & JESSIE JACOB, CONNECTING THE INDO-PACIFIC: THE FUTURE OF SUBSEA CABLES AND OPPORTUNITIES FOR AUSTRALIA 5 (2024), https://www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia/ [https://perma.cc/9CEQ-KGLN] (detailing how even a few undersea cable faults can wreak havoc on connected nations, especially those with comparatively fewer cables).

[5] *See* Kevin Frazier, *Wired for Failure: The Undersea Cable Emergency That Could Sink America's AI Aspirations*, LAWFARE (Sept. 16, 2025), https://www.lawfaremedia.org/article/wired-for-failure--the-undersea-cable-emergency-that-could-sink-america-s-ai-aspirations [https://perma.cc/ED9K-82PB] [hereinafter Frazier, Appendix A].

[6] Alan Mauldin, *Cutting off Europe? A Look at How the Continent Connects to the World*, TELEGEOGRAPHY:BLOG (Oct. 13, 2022), https://blog.telegeography.com/cutting-off-europe-a-look-at-how-the-continent-connects-to-the-world?utm_source=chatgpt.com [https://perma.cc/M2CM-AGP2]; *see* MIKE CONSTABLE ET AL., THE FUTURE OF SUBMARINE CABLE MAINTENANCE: TRENDS, CHALLENGES, AND STRATEGIES 34 (2025) [hereinafter FUTURE OF SUBMARINE CABLES], https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/The%20Future%20of%20Submarine%20Cable%20Maintenance_%20Trends%2C%20Challenges%2C%20and%20Strategies.pdf [https://perma.cc/7CQ2-Y26G] (forecasting as many of 25 trans-Atlantic cables by 2040).

alternative. Internet traffic travels drastically slower via satellites.[7] The satellite network also has significantly less bandwidth.[8]

This reality merits a two-prong response. The first is a "sea shot" that includes building 10 new cable repair ships explicitly for use by the nation's allies, deploying 100 autonomous undersea drones to gather critical information to maintain the undersea cable system, and laying or retrofitting 100,000 miles of undersea cables.[9] This prong is best thought of as an "offensive" strategy through which the US can reassert its authority in this critical domain. It will require significant political buy-in, financial support, and time. Cable operators often take years to lay a new cable.[10] Construction of a new undersea cable repair ship can take as many as five years.[11] Those delays mean that the US should pursue a second, "defensive" prong of this strategy in the interim. This strategy involves immediate adoption of policy strategies that deter bad actors from attacking the undersea cable system.

Increased Deterrence as an Immediate Priority

Deterrence is a function of three variables: the costs of an attack, the likelihood of its success, and the magnitude of its success. Bad actors will have little reason to attempt to sabotage the undersea cable system if doing so is expensive, difficult, or inconsequential. Critically, the same tools to deter intentional sabotage will also make the undersea cable system more resilient to the more frequent causes of cable faults, which also merit due consideration. As recommended by the International Cable Protection Committee (ICPC), undersea cable policy should be driven by evidence, not speculation or exaggeration.[12] Dragged anchors account for about 30 percent

[7] *Submarine Cable Frequently Asked Questions*, TELEGEOGRAPHY, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions [https://perma.cc/5LTQ-UMPE] (last accessed Nov. 17, 2025); INSIKT GRP, *Submarine Cable Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity*, RECORDED FUTURE (July 17, 2025), https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats [https://perma.cc/6VG5-UFP3] ("[A] trans-pacific fibre-optic call need only travel about 5,000 miles point-to-point, compared to a satellite call, which must travel 22,235 miles from the Earth to a satellite and then another 22,235 back.") (internal citation and quotation omitted).

[8] Alex Mauldin, *Will New Satellites End the Dominance of Submarine Cables?*, TELEGEOGRAPHY:BLOG (July 1, 2019), https://blog.telegeography.com/will-new-satellites-end-the-dominance-of-submarine-cables [https://perma.cc/3XP6-LXZC]; *The Battle for Bandwidth: Submarine Cable and Broadband Satellite Data*, NEW SPACE ECONOMY, https://newspaceeconomy.ca/2023/08/13/the-battle-for-bandwidth-submarine-cable-and-broadband-satellite-data/ [https://perma.cc/2GFT-TX2C] (last visited Nov. 17, 2025).

[9] *See* Frazier, Appendix A.

[10] *See* Jürgen Hatheier, *AI's role in revolutionizing submarine network connectivity*, RCR (Aug. 9, 2024), https://www.rcrwireless.com/20240809/network-infrastructure/ais-role-in-revolutionizing-submarine-network-connectivity-reader-forum [https://perma.cc/JA2W-D6QT] ("[T]hese are projects that cost in the hundreds of millions of dollars and take years to plan and deploy.").

[11] MIKE CONSTABLE ET AL., *supra* note 6, at 67.

[12] *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*, ICPC (last accessed Nov. 15, 2025) (on file with author).

of all breaks.[13] More generally, most breaks occur due to fishing and other human activities.[14] Any short-term solution should be evaluated under its responsiveness to both emerging issues, such as sabotage, as well as these more common causes of breaks.

Increasing the Cost of Sabotage

The costs of attacking submarine cables involve the actual expenses of locating and breaking a cable in addition to the probability of being caught multiplied by the punishment. New technologies, such as autonomous undersea vehicles or AUVs, will decrease the costs of an attack.[15] For sake of illustration, it appears as though Iran has already developed uncrewed undersea vehicles (UUVs) that are precisely designed to attack static targets.[16] What's more, Iran may have already made those tools available to the Houthi militant group.[17] Aerial drones have already transformed terrestrial conflicts by lowering the cost of destruction.[18] Iranian advances and their willingness to pass technology along to non-state actors suggests the same may be true in the undersea domain—to the extent it is not already.[19] The United States should respond by developing similar AUVs and UUVs—as called for under the "sea shot" described above, while also increasing its enforcement capabilities and punishments in the short run.

To start, Congress must amend the Submarine Cable Act of 1888 to minimally bring the fines for willfully or negligently breaking a cable in line with international norms and, ideally, to specify fines of an ever-greater magnitude. The current fines are $5,000 and $500, respectively.[20] It's likely cheaper to intentionally break an undersea cable than to go on a holiday trip to Europe. In contrast, New Zealand imposes a $120,000 penalty on any person who breaks a cable

---

[13] *Damage to Submarine Cables from Dragged Anchors*, ICPC: VIEWPOINTS (Feb. 24, 2025), https://www.iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/ [https://perma.cc/Q4RX-XPPP] [hereinafter *Dragged Anchors*]

[14] SUBMARINE TELECOMS F., *Year in Review*, 14 SUBMARINE TELECOMS INDUS. REP., at 166 (2025) [hereinafter INDUSTRY REPORT].

[15] JOINT COMMITTEE ON THE NATIONAL SECURITY STRATEGY, SUBSEA TELECOMMUNICATIONS CABLES: RESILIENCE AND CRISIS PREPAREDNESS, 2024-26, HC 723/HL 179, at 10 (UK); *see id.* at 14 (citing Professor Rowlands' observation that advances in AUVs may increase the odds of attacks on multiple cables at once); Yuval Eylon, *The Challenge of Defending Underwater Communication Infrastructures*, INSS (June 29, 2023), https://www.inss.org.il/publication/under-water/ [https://perma.cc/96RY-RRU2] (warning of "[r]ecent state-of-the-art developments of underwater capabilities, such as long-range midget unmanned submersible vehicles and remotely controlled submarine robots[.]").

[16] Ash Rossiter, *Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs)*, 171 MARINE POL'Y, Jan. 2025, at 1, 1–5.

[17] *Id.*

[18] *See, e.g.,* James Paterson, *High-tech drones are changing warfare – terrorists may soon follow the same playbook*, THE CONVERSATION (Aug. 12, 2025), https://theconversation.com/high-tech-drones-are-changing-warfare-terrorists-may-soon-follow-the-same-playbook-262626 [https://perma.cc/N6BM-VEJU].

[19] Margo Anderson, *Protecting Undersea Internet Cables Is a Tech Nightmare*, IEEE (Dec. 5, 2024), https://spectrum.ieee.org/undersea-internet-cables-protection-tech [https://perma.cc/U2KR-3P4Y].

[20] 47 U.S.C. § 22.

regardless of their intent.[21] Singapore has imposed a penalty on that scale, too;[22] in 2022, a private construction company faced $220,000 in fines for causing multiple telecommunication cables to break while working on a nearby project.[23] Australia may impose fines of nearly $27,000 for related offenses.[24] The United States should not dilly-dally in updating the Submarine Cable Act and sending a strong signal that it is ready and willing to hold bad actors accountable for their interference with this critical infrastructure. Many of the undersea cable breaks attributed to nations such as China and Russia have been carried out by commercial vessels in relatively shallow waters[25]—breaks that may fall within ambit of the Submarine Cable Act if committed near the US coast.

Increasing the Odds of Detection

To increase the odds of detecting responsible parties, Congress should condition any grant or renewal of a cable landing license upon the cable operator installing the latest sensing technologies and timely reporting any threats or anomalous activity. In the alternative, the cable operator can agree to a greater licensing fee to contribute to the ability of the US Government, including but not limited to the Coast Guard,[26] to track ships, submarines, and AUVs and UUVs. As an aside, fees collected by licensing authorities around the world should be explored as a means to gather funds necessary to solve some of the collective action problems that plague the undersea cable system.[27]

Every cable operator must secure a license from the Federal Communications Committee (FCC) prior to landing a cable in the US.[28] Applicants must provide relatively little information to the FCC to satisfy statutory obligations.[29] Certain applications receive heightened scrutiny by the FCC and a number of other agencies with an interest in the nation's telecommunications

---

[21] *Protecting New Zealand's Undersea Cables*, MINISTRY TRANSP., https://www.transport.govt.nz/about-us/what-we-do/queries/protecting-new-zealands-undersea-cables [https://perma.cc/CM8M-B3MH] (last visited Nov. 17, 2025)
[22] William Yuen Yee, *Laying Down the Law Under the Sea: Analyzing the US and Chinese Submarine Cable Governance Regimes*, JAMESTOWN (Aug. 4, 2023), https://jamestown.org/laying-down-the-law-under-the-sea-analyzing-the-us-and-chinese-submarine-cable-governance-regimes/ [https://perma.cc/WE83-J4CA].
[23] *Id.*
[24] *Id.*
[25] John Dotson, *Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations*, JAMESTOWN (June 7, 2025), https://jamestown.org/strangers-on-a-seabed-sino-russian-collaboration-on-undersea-cable-sabotage-operations/ [https://perma.cc/BQ77-N3JC].
[26] *Cf.* Madison L. Long, *Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks*, U.S. NAVAL INST. (May 2023), https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks [https://perma.cc/9WTN-GEF5] (contending that the Coast Guard should lead in efforts to protect the undersea cable system).
[27] Kevin Frazier, *Pooling Responsibility: Incentivizing Cable Owners to Safeguard the Global Undersea Network*, SSRN (Nov. 11, 2025) (forthcoming UNIV. CINN. L. INTELL. PROP. COMP. L.J.) [Appendix B].
[28] 47 CFR § 1.767.
[29] *Id.*

network—collectively known as "Team Telecom."[30] This group broadly examines whether granting a license would "pose[] a risk to national security or law enforcement interests of the United States."[31]

Even under this heightened review, it's unclear if Team Telecom will surface meaningful information about an operator's plans to adopt specific safeguards and to share specific information. For example, while applicants must answer, "What provision will be made to monitor suspicious activity occurring over the paths of the cables?",[32] the response may not detail the information called for here. It's also not clear whether the applicant's answer to that question would be determinative in the decision to grant, renew, or deny a license. Though the FCC is in the process of amending and streamlining this process,[33] decisions by Team Telecom have been faulted as unpredictable for relying on a seemingly shifting set of standards and information.[34] Amid these reform efforts, the FCC—at the direction or encouragement of Congress—should factor this information into its review of all licenses.

Myriad new technologies can generate important information from undersea cables. Quantum sensing, for example, "could transform subsea cable monitoring by enabling accurate detection of environmental changes, underwater seismic activity, and potential threats like fishing trawls or sabotage."[35] Acoustic sensors may perform a similar function.[36] A German company has even developed a means to update existing cables with sonar-like technology that can determine if threats are nearby by "sens[ing] vibrations traveling through the water[.]"[37] Deciding which of these sensing technologies should be imposed on applicants warrants additional analysis by the FCC based on their costs and accuracy. The key is that "dumb" cables that provide little to no information to the operator and government become a thing of the past. Any information gathered by the sensors, such as any indications as to the current functionality of

[30] Exec. Order No. 13,913, 85 Fed. Reg. 19643 (Apr. 8, 2020) (Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector).
[31] *Id.* at 19645
[32] Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, Second Report and Order, 36 FCC Rcd. 14848, 14873 (2021), https://docs.fcc.gov/public/attachments/FCC-21-104A1_Rcd.pdf [https://perma.cc/L8H5-43EV].
[33] Ari Fitzgerald et al., *FCC issues submarine cable rules, seeks comment on additional proposals*, HOGAN LOVELLS (Sept. 16, 2025), https://www.hoganlovells.com/en/publications/fcc-issues-submarine-cable-rules-seeks-comment-on-additional-proposals [https://perma.cc/6GX2-JU4G].
[34] RICHARD SALGADO, UNDERSEA CABLES, HYPERSCALERS, AND NATIONAL SECURITY 9 (2023).
[35] Devon A. Johnson, *INTO THE FUTURE: Quantum Technologies and the Impact on the Resilience of the Subsea Cable System*, SUBMARINE TELECOMS FORUM (Dec. 2, 2024), https://subtelforum.com/into-the-future-quantum-technologies-and-the-impact-on-the-resilience-of-the-subsea-cable-system/ [https://perma.cc/Q9TL-2MVC].
[36] *OPTODAS: The Leading Technology for Distributed Acoustic Sensing*, ASN, https://www.asn.com/fiber-sensing [https://perma.cc/C7MM-KMWY] (last accessed Nov. 17, 2025) (ASN opens a new era in subsea intelligent sensing based on advanced DAS technology).
[37] Jowi Morales, *New undersea cable tech listens for sabotage — can be retrofitted to existing fiber optic lines*, TOM'S HARDWARE (Mar. 18, 2025), https://www.tomshardware.com/tech-industry/new-undersea-cable-tech-listens-for-sabotage-can-be-retrofitted-to-existing-fiber-optic-lines [https://perma.cc/DX5M-KZ4D].

the cables,[38] then needs to be passed along to the relevant government authorities. Provision of more information about cables can inform ongoing policy decisions about how to increase the resiliency of the undersea cable system—decisions that are often made in the absence of full information.[39]

These two straightforward steps will alter the calculus of bad actors who often turn to commercial vessels to carry out attacks on their behalf. A more ambitious, though necessary step involves designating cable protection zones, which would prohibit activities that interfere with the seabed from occurring in specified areas with a high density of cables.[40] Australia,[41] New Zealand,[42] and Denmark[43] are among the nations with such zones. The efficacy of this strategy turns on whether the State allocates sufficient enforcement resources to what may be a very difficult task of monitoring several zones. The United States could start by creating cable protection zones where there is already a high number of cables in a relatively finite geographic area. One place to start may be the North Coast of Oregon. At least eight trans-Pacific cables go through that area.[44] This area is also forecasted to be especially prone to breaks in the coming years.[45] A combination of the Coast Guard, Air Force, Navy, and other authorities with resources to closely monitor ship traffic in that region could ensure a high enough degree of enforcement so as to deter bad actors from even attempting to sabotage those cables. Technological advances such as AI may make this monitoring all the easier[46] and justify creating such zones in other areas.[47]

Reducing Odds of Success

[38] *See* JOCELINN KANG & JESSIE JACOB, supra note 4, at 21 (recommending that Australia likewise mandate the provision of such information).
[39] *See, e.g.,* JOINT COMMITTEE ON THE NATIONAL SECURITY STRATEGY, *supra* note 15, at 2 (highlighting the fact that additional information on how cable damage impacts cable operations would assist policy discussions).
[40] *See* Pierre Thévenin, *A legislative route to combat sabotage of undersea cables: A Q&A with Pierre Thévenin*, SIPRI (Oct. 23, 2025), https://www.sipri.org/commentary/topical-backgrounder/2025/legislative-route-combat-sabotage-undersea-cables [https://perma.cc/352U-NBUG] (including bottom trawling, dredging, and anchoring among such activities).
[41] Telecommunications Legislation Amendment (Submarine Cable Protection) Bill 2014 (Cth) (Austl.).
[42] Submarine Cables and Pipelines Protection Act 1996 (N.Z.).
[43] Order no. 939 of 27 November 1992 on the protection of submarine cables and submarine pipelines (Den.).
[44] *Submarine Cable Map*, TELEGEOGRAPHY, https://www.submarinecablemap.com [https://perma.cc/B87F-89UQ] (last accessed Nov. 17, 2025).
[45] FUTURE OF SUBMARINE CABLES, *supra* note 6, at 51–52.
[46] Matthew Kastler, *Move Beyond AIS for Maritime Domain Awareness*, U.S. NAVAL INST. (Sept. 2025), https://www.usni.org/magazines/proceedings/2025/september/move-beyond-ais-maritime-domain-awareness [https://perma.cc/M8W6-MLMT].
[47] *See* Kevin Frazier, *Policy Proposals for the United States to Protect the Undersea Cable System*, 13 CASE W. RSRV. J.L. TECH. & INTERNET, no. 1, 2022, at 30–32 (2022) (identifying the high number of undersea cables across two coasts as a barrier to the United States adopting cable protection zones) [Appendix C].

Congress can also drastically diminish the likelihood of a successful attack by imposing heightened responsibilities on cable operators to adopt best practices for laying more attack-resistant cables. The vast majority of cable breaks occur in shallow water, near shore, and in cable choke points.[48] Cable operators can implement several safeguards against such breaks. First, they can increase the armoring of cables.[49] Use of Kevlar to safeguard cables from sharks and other threats was once regarded as a novel tactic,[50] though its use has since spread.[51] New materials may soon promise even greater protection while not unduly burdening the cost and operational difficulties of coiling, then unspooling cables as they're laid on the seafloor.[52] The FCC should expect that operators are continuously studying the availability of superior armoring and justifying to what extent they do or not use it.

Second, operators can bury cables at a greater depth and further from the coast. As it stands, the norm is that cables lie on the surface when at a depth of 100 meters or more.[53] This means that in some deepwater ports and high trafficked areas cables may be especially susceptible to sabotage.[54] Operators could additionally be obligated to at least consider the need to use mattress covering around the cable and assess the placement of nearby rocks, which may shift due to currents.[55]

Third, operators can adhere to minimum separation standards to distance their cables from others. Additional spacing between cables can reduce the odds of single incidents causing numerous breaks. By way of example, in 2008, a single ship damaged six cables due to

---

[48] *See* NATO COOP. CYBER DEF. CTR. EXCELLENCE, STRATEGIC IMPORTANCE OF, AND DEPENDENCE ON, UNDERSEA CABLES 3 (2019) [hereinafter NATO REPORT], https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf [https://perma.cc/98RV-46DK] (warning that terrorists are most likely to attack cables near cable landing stations).

[49] CAMINO KAVANAGH, WADING MURKY WATERS, UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH 12 (2023), https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Wading_Murky_Waters_Subsea_Communications_Cables_Responsible_State_Behaviour.pdf [https://perma.cc/3ZP9-T4R7]; James Griffiths, *The global internet is powered by vast undersea cables. But they're vulnerable*, CNN (July 26, 2019), https://www.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk [https://perma.cc/8KSY-BLXN].

[50] NATO REPORT, *supra* note 48, at 3; Will Oremus, *The Global Internet Is Being Attacked by Sharks, Google Confirms*, Slate (Aug. 15, 2014), https://slate.com/technology/2014/08/shark-attacks-threaten-google-s-undersea-internet-cables-video.html [https://perma.cc/CX8D-4T3S].

[51] James Griffiths, *supra* note 49.

[52] *See* Darren Orf, *Scientists Created a Bulletproof Material 3 Times Stronger Than Kevlar—It's Already Breaking Records*, POPULAR MECHANICS (Nov. 11, 2025), https://www.popularmechanics.com/science/a69268884/carbon-nanotube-kevlar/ [https://perma.cc/ZF4T-QZS2].

[53] Alex Botting & Inés Jordan-Zoob, *How the US and its Partners can Ensure the World's Data Super-Highways Remain Reliable, Secure, Open & Free*, WILSON CTR. (July 15, 2024), https://www.wilsoncenter.org/article/how-us-and-its-partners-can-ensure-worlds-data-super-highways-remain-reliable-secure-open [https://perma.cc/T2CJ-MMYJ].

[54] *Id.*

[55] *The JRC explains: Subsea cables: how vulnerable are they and can we protect them?*, Joint Rsch. Ctr. (Aug. 8, 2025), https://joint-research-centre.ec.europa.eu/jrc-explains/subsea-cables-how-vulnerable-are-they-and-can-we-protect-them_en [https://perma.cc/B3D5-T6PT].

dragging its anchor along the seafloor.[56] Some degree of spacing can make it less likely that one net, anchor, rock, or UUV can break several cables at once.

Fourth, in the event Congress creates cable protection zones, operators can lay cables in those zones to ease the task of monitoring threats to cables. As the requisite authorities closely monitor these specific areas, they can quickly mobilize the forces necessary to stop a bad actor from "lingering" in that zone as that actor attempts to break several cables in quick succession.

Each of these measures will frustrate efforts by bad actors to cause significant and prolonged outages. Operators that opt not to adhere to these defensive measures should again face heightened licensing fees.

Diminishing the Damage from a Successful Attack

In the event that a bad actor manages to break a cable or, in a worst-case scenario, several cables, deterrence calls for policies that ensure network redundancy and rapid repair times. Put differently, adversaries will have less interest in attacking cables if traffic can easily be routed through other cables and damaged cables can be restored in days rather than weeks or months. A case study makes this point clear. When a series of minor accidents caused damage to several cables off the coast of Côte d'Ivoire, many Internet users across Africa experienced diminished service.[57] Comparatively, when two cables broke in the Baltic Sea, users experienced few to no issues because of the availability of alternative routes for Internet traffic.[58] That's precisely why redundancy is a key part of a robust undersea cable system.[59]

A redundant undersea cable system includes a number of cables being laid along diverse routes. Congress should study various financial levers to support ongoing cable building both by the US and its allies, especially in regions that will see many existing cables be retired in the coming years. A survey of industry stakeholders suggests that more than 800,000km of cables will be retired by 2040.[60] As cables reach the end of their operational or economic lives, the US must pay attention to whether their allies are at a heightened risk of being susceptible to prolonged Internet outages due to just a few breaks.[61]

---

[56] *Dragged Anchors*, *supra* note 13.
[57] Paula Gilbert, *Multiple cable failures impact Africa's Internet*, CONNECTING AFR. (Mar. 15, 2024), https://www.connectingafrica.com/connectivity/multiple-cable-failures-impact-africa-s-internet [https://perma.cc/CV2U-3PFD].
[58] David Belson, *Resilient Internet connectivity in Europe mitigates impact from multiple cable cuts*, CLOUDFLARE:BLOG (Nov. 11, 2024), https://blog.cloudflare.com/resilient-internet-connectivity-baltic-cable-cuts/ [https://perma.cc/384B-86UZ].
[59] INSIKT GRP, *supra* note 7.
[60] FUTURE OF SUBMARINE CABLES, *supra* note 6, at 2.
[61] *See, e.g.,* Commission Recommendation (EU) of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures, 2024 O.J. (L779) at 1 (warning that some members of the EU may already be in such a position).

While hyperscalers are racing ahead with their own cable projects, the United States has an interest in ensuring redundancy across the entire system.[62] If Google, Amazon, and other hyperscalers do not see an economic case for filling in gaps in the undersea cable system, it's unlikely other private actors will fill the void. Cable laying is a gamble. Only about half of announced undersea cable projects get completed.[63] An increasingly bifurcated and concentrated supply chain is only making such projects costlier.[64] For all those reasons, it's pivotal that allies look to the United States and not China to increase their own cable connections.

Most importantly, the US must ensure that any successful disruptions to a cable or cables are short-lived. This is yet another cost-intensive and logistically difficult task. Average repair times have varied over the last few years—taking nearly three months in 2022 (78 days) while falling to about a month (32 days) in 2025.[65] As the number of cables increases over the next decade[66] and the number of cable repair ships in need of replacement surges,[67] a betting man would like the odds that the average undersea cable repair time is increasing. This will be especially true if a repair is required during a geopolitical conflict. One industry observer expected that a cable repair ship would demand a military escort prior to sailing to the repair point.[68]

Congress should swiftly pass legislation like the Neptune Act that aims to bolster the number of cable repair ships.[69] The number of cable repairs is forecasted to reach 287 by 2040.[70] Our cable operators should not have Chinese ships on speed dial to patch cables carrying our sensitive communications. Nor should US cable providers expect cable repair ships flying another nation's flag to prioritize repairs to US cables over their own.[71] This is and must be a problem solved by US ships. We're woefully behind on this front.

Minimally, Congress should amend the cable landing license to mandate that operators have at least a ten-year contract with a cable repair provider. This shift would address the financial uncertainty that often prevents cable repair ship owners from further investing in their fleets.

---

[62] JOCELINN KANG & JESSIE JACOB, *supra* note 4, at 7 (estimating that hyperscalers such as Google, Meta, Microsoft, and Amazon have had at least some stake in nearly 25 percent of all undersea cable projects that launched between 2019 and 2023).
[63] Big tech and geopolitics are reshaping the internet's plumbing, ECONOMIST (Dec. 20, 2025), https://www.economist.com/business/2023/12/20/big-tech-and-geopolitics-are-reshaping-the-internets-plumbing.
[64] JOCELINN KANG & JESSIE JACOB, *supra* note 4, at 10–12.
[65] FORUM INDUSTRY REPORT, *supra* note 14, at 100.
[66] FUTURE OF SUBMARINE CABLES, *supra* note 6, at 47.
[67] *Id.* at 61.
[68] JOINT COMMITTEE ON THE NATIONAL SECURITY STRATEGY, *supra* note 15, at 24.
[69] Press Release, Max Miller, Congressman Max Miller Introduces NEPTUNE Act to Protect America's Critical Infrastructure (July 25, 2025), https://maxmiller.house.gov/posts/congressman-max-miller-introduces-neptune-act-to-protect-americas-critical-infrastructure [https://perma.cc/4NGA-8YBT].
[70] FUTURE OF SUBMARINE CABLES, *supra* note 6, at 50.
[71] *See* JOINT COMMITTEE ON THE NATIONAL SECURITY STRATEGY, *supra* note 15, at 25 (expecting French cable repair ships to respond to cables of French significance over cables of importance to the UK).

Conclusion

The US is entering an era in which AI will amplify every facet of national power—from scientific research and economic productivity to military readiness and diplomatic leverage. But AI's promise is only as strong as the physical infrastructure that undergirds it. Undersea cables are not a peripheral issue in the AI age. Instead, Congress must regard the undersea cable system as a foundational part of the emerging global economy. If these cables are compromised, our most advanced AI labs, high-performance computing clusters, and data-rich enterprises will be unable to operate at the scale that global leadership demands. Congress must therefore treat cable resilience not as a niche maritime concern but as a foundational pillar of American competitiveness.

Though Congress should move forward with a "sea shot" over the long term, a focus on deterrence in the short run can collectively reshape the incentives of adversaries and limit the consequences of disruptions. But as AI systems become more central to real-time intelligence analysis, financial markets, precision agriculture, disaster response, and critical infrastructure management, even brief outages will impose cascading harms. A cable system built for the pre-AI era—an era of slower data flows, fewer real-time applications, and limited global compute—cannot meet the demands we now face. Policymakers must recognize that strengthening undersea infrastructure is not just about preventing sabotage; it is about ensuring that the nation can fully leverage AI to enhance the well-being and security of every American.

Ultimately, Congress has a rare opportunity to act before a crisis forces its hand. The investments and policy changes proposed here will not only strengthen our undersea cable network but also secure the connective tissue of the AI economy for decades to come. With deliberate action—guided by deterrence, informed by evidence, and executed with urgency—the US can ensure that its cables, like its AI ambitions, are resilient, adaptive, and firmly under American control.

APPENDIX A

LAWFARE

Cybersecurity & Tech

Wired for Failure: The Undersea Cable Emergency That Could Sink America's AI Aspirations

Kevin Frazier

Tuesday, September 16, 2025, 9:55 AM

The undersea cable system faces threats from deep-sea mining, geopolitical sabotage, and AI-driven demand, requiring immediate federal action.

The artificial intelligence (AI) dominance the White House called for in its recently released AI Action Plan is not going to happen unless the president, Congress, and the country get serious about protecting the undersea cable system—the 600 or so inch-wide cables over which the world's internet traffic flows. A combination of natural and human threats imperil the resilience of this critical infrastructure just as AI advances make the cables more essential than ever. Though the plan included 90 recommendations, including several massive infrastructure projects to sustain continued AI development, it also had approximately 600 garden-hose-sized holes—an omission with large political, economic, and technological ramifications.

A recently announced proposed rule by the Federal Communications Commission (FCC) to expedite review of cable licenses, if finalized, is a step in the right direction. The licensing process is a key bottleneck in laying and retrofitting undersea cables. Private actors rely on predictable and efficient approval to move forward with costly projects, which makes the FCC's proposed rule all the more important and timely. However, it likely will fall short of the leap in cable development that's required to match the magnitude of the threat facing this critical infrastructure. Around 100,000 miles of new cables are necessary by 2040 to meet expected internet traffic demands. Prior efforts to streamline licensing have experienced mixed results. Under the current system "a 120-day review often takes closer to six to eight months," according to one participant. Until the final text of the rule is made clear, it is uncertain whether such delays will become a

thing of the past. Moreover, the proposed rule does not significantly address several of the most significant concerns facing the undersea cable system, such as the need for drastically more cables, improved cable quality, and far more monitoring of the ocean floor.

Nearly 100 percent of intercontinental internet traffic travels through narrow undersea cables. Diverting that traffic to space isn't a viable alternative since information flows five times faster via cables than satellites. Put simply, the cables are the internet plumbing the world has come to rely on. Whether those pipes endure for the next decades and beyond is an open question as they deteriorate due to strong currents, sea creatures, and normal wear and tear and continue to be the targets of bad actors. The president and Congress need to take immediate action if they want to avoid their AI dominance aspirations being thwarted due to an overlooked critical infrastructure.

The Building Threat to Undersea Cables

Three developments are making the already-brittle undersea cable system all the more susceptible to interference. First, the Trump administration has significantly lowered barriers to mining deep-sea minerals in American waters as well as the high seas. Other countries have either facilitated this unprecedented commercial activity or seem likely to follow in America's footsteps by initiating projects of their own.

A surge in deep-sea activity—moving rocks, dropping equipment, and so on—will pose a grave threat to the garden-sized hoses that crisscross the oceans. The vast majority of cable breaks occur due to natural causes and human error. Deep-sea mining will presumably make those breaks more common. Cables are not exactly resilient to physical damage. A shark, a fishing net, an anchor, and even a rock moving in the wrong way at the wrong time can sever a cable. Mining promises to introduce a heightened degree of uncoordinated activity on the sea floor, especially considering that the National Oceanic and Atmospheric Administration is on its way to streamlining the mining permitting process and companies have shown a willingness to ignore the guidance of the International Seabed Authority, an autonomous international organization created by the 1982 United Nations Convention on the Law of the Sea.

Second, the explosion in AI use is at once making access to high-speed internet more important and more scarce as increased traffic clogs technical systems suited to a different era. The battle among private and public stakeholders to build out the physical infrastructure associated with AI dominance may soon move under the seas. Private AI labs, such as Meta, are already rushing to lay new cables to keep pace with current and forecast demand. Who builds which cables and for what countries is a hotly contested and highly consequential matter. Adversaries have plenty of reason to attempt to delay or undermine massive cable initiatives

such as Meta's Project Waterworth, which will span five continents and account for approximately 31,000 miles in cable. Setbacks to such resource intensive endeavors may ripple across a nation's entire tech stack due to diminished high-speed internet access. What's more, as the undersea cable system itself expands, the institutions and actors tasked with its maintenance and repair will become even further stretched thin. As it stands, no entity or collection of entities meaningfully monitors all 870,000 miles of undersea cables.

Third, there appears to be no end in sight to geopolitical tensions that adversaries have cited as an excuse to disrupt the undersea cable system. In the past year or so, six cable breaks have been attributed to China and Russia. The Houthis may have cut four cables in 2024. Advances in undersea drones and related naval technologies will allow adversaries to commit such acts at greater depths with greater frequency and with even lower odds of attribution. Suddenly the 17 or so cables connecting North America to Europe seems like an awfully low number.

Proposals Reflective of the Value of the Undersea Cable Systems

To be fair to a number of scholars, such as David Opderbeck, and politicians, including former U.K. Prime Minister Rishi Sunak and Sens. Chris Murphy (D-Conn.) and Todd Young (R-Ind.), who have proposed policy ideas, several important stakeholders have recognized and attempted to address the fragility of the undersea cable system. Their solutions, however, have often been too reliant on international law frameworks with low odds of successful enforcement or too meager to result in a substantially more resilient undersea cable system. One of Sunak's main proposals—an international treaty—is likely a nonstarter in today's geopolitical environment. What's more, Congress is currently weighing legislation that would build two new submarine cable-laying and repair ships. That's akin to the New York City Council touting two new ambulances. It's just not enough to make a real difference.

Cable repair work poses unique challenges. Bad weather, a shortage of talented workers, and a dearth of boats all mean that in the event of several cables breaking it will take weeks, if not months, to get them back on line. That was the case a few years back when it took six months to repair four cables off the coast of Vietnam. Similarly, in 2006, when an earthquake broke six of the seven cables near the Luzon Strait, it took 11 ships 49 days to bring the cables back on line.

Solutions that have worked in other contexts likewise seem ill-suited to the nature and scale of the crisis facing the undersea cable system. New Zealand, for example, has implemented cable protection zones that limit naval traffic near areas with cable clusters. The government has committed significant resources to enforcing those zones. So far, these zones seem to have worked. But it's important to note that these zones likely benefit from having a drastically smaller number of cables (just four) in a narrower geographic area than a nation like the United States.

It is time for far more drastic action grounded in two core principles—redundancy and resiliency—and three proposals: 10 new cable repair ships, 100 autonomous undersea drones, and 100,000 miles of new or retrofitted undersea cables—or the "10-100-100,000 initiative."

On redundancy, the president should apply his "America First" approach to governance by seeking to become the first president to lay 100,000 miles of undersea cables. It's a big number. He likes setting big goals. Why not aim for the sky? (Or the depths?) Whereas three state-owned Chinese firms are actively extending that country's ambitions via new cables, the U.S. government—specifically, the Navy—owns just 40,000 miles of cable. The goal would be to lay many more cables between the U.S. and key overseas markets as well as to replace or retrofit cables at risk of diminished capabilities due to age. Ideally, the government would partner with existing cable owners to do so given their expertise and existing infrastructure. However, it may also want to independently build some of those cables given the importance of not relying solely on private entities for the maintenance of this critical infrastructure. As the number of cables grows, the net harm of an attack on any one cable diminishes; traffic can be fairly easily rerouted. This bold endeavor also amounts to good policymaking. Many cables laid near the early days of the internet are reaching the end of their typical life cycle of approximately 20 years. The combined need for a more redundant system and one that is suited to the AI age makes this effort all the more important.

Extensive executive power could aid the president in realizing this aquatic moonshot (dare I say, "sea shot"). In line with several recommendations in the AI Action Plan, the president can lower regulatory hurdles to laying cables and establishing cable landing points on shore. A litany of federal agencies, including the National Oceanic and Atmospheric Administration and the Federal Communications Commission, play a role in determining which individuals can do what in and around the ocean. The cumulative result can bring undersea cable development to a halt. Washington state, despite its proximity to Asia, has not been the site of a new cable connection point in more than two decades; local, state, and federal hurdles may be to blame. The slow and, in some cases, seemingly arbitrary denial of cable licenses by Team Telecom—an advisory body to the FCC made up of the Departments of Justice, Defense, and Homeland Security—deserves particular scrutiny. Team Telecom's recommendations to the FCC as to whether to approve or deny a license are often determinative, yet commonly turn on ad hoc considerations. The resulting uncertainty has unsurprisingly drawn the ire of cable owners. Proposed FCC rules to accelerate this process may assuage some of these concerns but may stop short of addressing some of the aforementioned state and local barriers.

What's more, the president can leverage the Defense Production Act (DPA) to ease the burden of securing the materials necessary to lay that many cables. The current supply chain is highly fragmented and involves several scarce, expensive inputs. Cables are the product of parts assembled by dozens, if not hundreds, of companies. The DPA is a tool tailored to remedying those sorts of barriers. Pursuant to its expansive provisions, the president may mandate that federal production and supply contracts receive priority and direct private actors to expand production of certain goods. DPA authorities are contingent on the president acting with an eye toward national defense. That should not pose a problem here given that both commercial and military communications rely on a durable undersea cable system.

On resiliency, the construction and deployment of 10 additional cable repair ships and 100 autonomous undersea drones capable of monitoring adversary ships and drones as well as assessing the durability of cables will go a long way toward helping Americans get back on their feet by getting back online in the event of a sizable attack on the undersea cable system. The value of additional cable repair ships has already been explored and is fairly obvious. Autonomous undersea drones, however, would constitute a novel but overdue investment. New sea drones, such as those created by Germany-based Helsing, can remain underwater for up to four months and clandestinely surveil enemy ships.

Thankfully, the Navy is already soliciting input from the private sector on how to develop and deploy drones with similar capabilities as soon as possible. This effort should include an expectation that the drones be capable of both detecting threats to undersea cables and, critically, pinpointing where a cable has been severed. By championing this nascent effort through the announcement of the 10-100-100,000 initiative, President Trump may be able to scale up the level of congressional support for its continuation as well as to attract more private-sector interest.

***

The undersea cable crisis represents more than a technical challenge—it embodies the tension between America's digital aspirations and the physical realities that underpin them. Just as the transcontinental railroad required bold federal action to connect a divided nation, today's digital infrastructure demands similar vision and commitment. The fragility of our current system reflects a broader pattern in American governance: the tendency to build magnificent superstructures while neglecting the foundations that sustain them.

The 10-100-100,000 initiative offers more than redundancy and resilience—it presents an opportunity to reclaim American leadership in the infrastructure that will define the next century of global competition. History suggests that nations that control the arteries of communication wield disproportionate influence over

the flow of information, commerce, and, ultimately, power itself. The British Empire's telegraph cables, America's satellite networks, and now China's Digital Silk Road initiative all demonstrate this enduring truth.

Yet the path forward requires acknowledging an uncomfortable reality: America's adversaries have recognized the strategic value of undersea cables while the U.S. government has treated them as utilities rather than a key feature of our national defense. The garden-hose comparison is apt not merely for its physical dimensions, but for how policymakers have conceptualized these vital arteries—as mundane infrastructure rather than the nervous system of American digital dominance.

The president's opportunity is clear. By framing undersea cable expansion as both economic necessity and national security imperative, he can marshal the same political energy that built interstate highways and put Americans on the moon. The ocean floor awaits America's next great infrastructure project. The question is whether the United States will seize this moment or allow others to write the rules of our digital future from the depths below.

Kevin Frazier

𝕏 @kevintfrazier

kevintfrazier.bsky.social

Read More

Kevin Frazier is an AI Innovation and Law Fellow at UT Austin School of Law and Senior Editor at *Lawfare*.

}

APPENDIX B

Pooling Responsibility: Incentivizing Cable Owners to Safeguard the Global Undersea Network

Kevin Frazier
AI Innovation and Law Fellow
The University of Texas School of Law

ABSTRACT

Undersea cables form the backbone of the global communications system, yet the legal regimes governing their installation, maintenance, and protection remain fragmented, reactive, and ill-suited to the mounting risks facing this infrastructure. Existing frameworks diffuse responsibility across states, agencies, and private owners, creating a system in which even straightforward incidents trigger jurisdictional confusion, duplicative inquiries, and costly delays. The result is a structural misalignment: governments bear the burdens of resilience while the cable owners best positioned to prevent and rapidly repair breaks face minimal obligations. This Article argues that a durable legal architecture requires reversing that allocation of responsibility.

Drawing on the shortcomings of the United States' multilevel regulatory landscape—exemplified by Team Telecom's inconsistent and protracted licensing reviews—this Article demonstrates how the current model elevates cable-by-cable adjudication at the expense of system-wide resilience. It proposes a new regulatory paradigm that conditions landing rights on operator participation in a resilience pool: a shared fund capitalized by annual contributions calibrated to each operator's risk profile, performance history, and adoption of best practices. Unlike traditional insurance, the pool rewards prevention, redundancy, continuous monitoring, and transparent reporting through predictable incentive structures; it also supports rapid repair, shared information systems, and long-term technological upgrades.

By shifting accountability upstream to cable owners and embedding resilience obligations in the licensing process, this approach corrects the core market failure—underinvestment in a global public good—and replaces fragmented adjudication with a coherent, systemic orientation. A pooled model ensures that outages are addressed immediately, disputes are resolved after service is restored, and private incentives finally align with the public interest in maintaining a secure, stable, and future-ready undersea network.

Hypothetical: If a fishing vessel registered in Country A, whose crew members are nationals of Country B, damages a submarine cable owned by a telecommunications company registered in Country C, in the high seas near Country D, where one end of the cable lands, how should this case be treated?

The complicated, fragmented, and incomplete set of local, national, international, and private laws applicable to the undersea cable system make even the most straightforward hypothetical undersea cable incident a challenging legal exercise.[1] An incident involving a ship from Country A that is manned by individuals from Country B and a cable owned by a company in Country C that is severed in the high seas of Country D invites a seemingly endless set of inquiries.

A brief review of just a handful of those questions reveals the near impossibility of a simple legal resolution to a hypothetical that, at least on the surface, seems addressable under existing laws.

With respect to the ship: has it always flown the flag of Country A? For how long? Has it ever sailed under the flag of a different nation? What was the process like for flying under said flag or flags? Were those processes adhered to in this instance?

Regarding the individuals aboard the ship: are they naturalized citizens of Country B? What, if any, applicable legal obligations does Country B impose on them? Does Country B have a precedent of holding its individuals accountable for violations of any applicable laws?

Next, on cable ownership: is the company the sole owner of the cable or do other entities have a stake? If so, are those other entities also based in Country C? What agreements has the company made with Country D and any other countries that the cable connects to? Does the company have arrangements with other private actors to oversee different parts of the cable product journey—from laying the cable to repairing breaks?

Consideration of the cable location raises even more questions: are there conflicting claims between Country D and another country over the high seas in question? How long has Country D claimed jurisdiction over that area and how closely has Country D policed it in recent history? Within Country D, which regulatory authority or authorities exercise jurisdiction over that area?

This hypothetical scenario also does not raise perhaps the most difficult set of questions—those surrounding attribution.[2] Undersea cables are prone to breaking absent any human intervention.

---

[1] Jill Goldenziel, *Law Can't Stop Submarine Cable Sabotage. Russia And China Know It.*, FORBES (Feb. 14, 2025), https://www.forbes.com/sites/jillgoldenziel/2025/02/13/law-doesnt-protect-undersea-cables-russia-and-china-know-it/ [https://perma.cc/GB25-MM2T].

[2] Aaron Bateman, *To keep the world's data flowing, countries need to quickly fix broken undersea cables*, BULL. OF THE ATOMIC SCIENTISTS (July 29, 2025), https://thebulletin.org/2025/07/to-keep-the-worlds-data-flowing-countries-need-to-quickly-fix-broken-undersea-cables/ [https://perma.cc/4ZCR-67QQ].

Deterioration due to time[3], swift currents[4], warmer seas[5], and interaction with the natural environment[6] can precipitate a break. Yet omitted from the hypothetical is any information about the recent marine geologic events such as landslides that have been the frequent culprit of cable breaks.[7] Nor does the hypothetical detail the extent to which the ship in question was accurately tracked and whether such tracking has been independently verified and broadly accepted by the applicable stakeholders.[8] It is also unclear where the ship is presently located and the extent to which it may be willing to sail to Country D to facilitate a more thorough investigation.[9]

Under the current legal paradigm in the United States each of these inquiries would necessitate clear answers. Compilation of those answers, however, would prove contentious, time-consuming, and resource-intensive. In this regard the U.S. is far from exceptional. Like other nations[10], several governing authorities[11] have competing and, in some cases, conflicting jurisdiction over undersea cables. By way of example, municipalities in the U.S. may impose ordinances that dictate landing station locations. Coastal states in the U.S. share jurisdiction over their respective 12-mile (nautical) territorial seas with the federal government.[12] Manifold federal agencies oversee and enforce a wide range of statutes pertaining to the nation's vast telecommunications network, including undersea cables.

Examination of just one effort to govern the undersea cable product journey—approval of licenses for cable landing stations by the Federal Communications Commission (FCC)—

---

[3] Alan Mauldin, *Is the Lifespan of a Submarine Cable Really 25 Years?,* TELEGEOGRAPHY: BLOG (Apr. 20, 2023), https://blog.telegeography.com/2023-mythbusting-part-2 [https://perma.cc/8DS5-LWBZ].
[4] The Biggest Threat to Subsea Cables, ULTRAMAPGLOB.: ABOUT US (Aug. 4, 2024), https://ultramapglobal.com/the-biggest-threat-to-subsea-cables/ [https://perma.cc/ZCD2-GMJN].
[5] Michael Clare, *Are Subsea Cables Feeling the Heat From Climate Change?*, INTERNET SOC'Y PULSE: BLOG (July 2, 2024), https://pulse.internetsociety.org/blog/are-subsea-cables-feeling-the-heat-from-climate-change [https://perma.cc/WE4C-3ZQY].
[6] Stephen Drew, *Causes of Cable Faults and Repairs in Regional Seas*, INT'L CABLE PROT. COMM., https://cil.nus.edu.sg/wp-content/uploads/2009/10/Causes_of_Cable_Faults_and_Repairs_in_Regional_Seas.pdf [https://perma.cc/XCZ6-YE56] (last visited Oct. 19, 2025).
[7] JANE MUNGA, BENEATH THE WAVES: ADDRESSING VULNERABILITIES IN AFRICA'S UNDERSEA DIGITAL INFRASTRUCTURE 7 (2025), https://carnegie-production-assets.s3.amazonaws.com/static/files/Munga_Undersea%20Cables-2025.pdf [https://perma.cc/8TL7-KUMW].
[8] *Chinese Ship Suspected of Cable Sabotage May Have Had Two AIS Devices*, THE MAR. EXEC. (Jan. 7, 2025), https://maritime-executive.com/article/chinese-ship-suspected-of-cable-sabotage-may-have-had-two-ais-devices [https://perma.cc/3C22-7UQN].
[9] Johan Ahlander & Anna Ringstrom, *Swedish authorities board ship seized over Baltic Sea cable breach*, REUTERS (Jan. 27, 2025), https://www.reuters.com/world/europe/swedish-authorities-board-ship-seized-over-baltic-sea-cable-breach-2025-01-27/ [https://perma.cc/BF39-9YEG].
[10] *Ocean and Coastal Jurisdiction*, W. Coast Env't L.: Programs & Campaigns, https://www.wcel.org/ocean-and-coastal-jurisdiction [https://perma.cc/R5SR-8XSX] (last visited Oct. 19, 2025).
[11] Kevin Frazier, *Policy Proposals for the United States to Protect the Undersea Cable System*, 13 CASE W. RSRV. J.L. TECH. & INTERNET, no. 1, 2022, at 1, 24–29.
[12] NICOLE T. CARTER ET AL., CONG. RSCH. SERV., R47648, PROTECTION OF UNDERSEA TELECOMMUNICATION CABLES: ISSUES FOR CONGRESS 4–6 (2023).

exemplifies how legal processes intended to increase the resiliency of the undersea cable system often backfire. The FCC has long been tasked with setting the terms of undersea cable licenses and reviewing applications for those licenses.[13] Increased awareness of the economic and national security implications of undersea cables led to the FCC involving more agencies in that process.[14] Recommendations from the Department of Defense, Department of Homeland Security, and Department of Justice, among other agencies, have significant sway over FCC determinations. The agencies involved in that process—collectively known as Team Telecom—take their time in reviewing applications.[15] Though the review is supposed to occur in just 120 days, it often takes twice as long due to agencies evaluating applications based on varying questions and subjecting them to arbitrary, shifting approval standards.[16]

This brief review of Team Telecom's well-intentioned, yet deeply flawed cable approval process demonstrates that comparatively "easy" decisions surrounding undersea cables can be frustrated by allocating legal authority to too many or the wrong set of legal actors. Returning to cable incidents akin to the one presented in the hypothetical, which may involve four or more nations, several private actors, and many more external inputs, it is worth questioning if an entirely different legal ecosystem may better facilitate a resilient undersea system.

The current paradigm treats resilience as a state responsibility while allowing the companies that actually design, build, and maintain the cables to escape with only minimal accountability. The result is a system in which governments are drawn into endless case-by-case disputes while the owners most capable of preventing and repairing breaks remain on the sidelines. A more durable framework requires turning that allocation on its head: cable owners must be made directly responsible for the resilience of the network as a whole, with states using their licensing authority to enforce that responsibility. By moving accountability upstream—onto the operators who control design choices, monitoring practices, and repair readiness—law and policy can finally shift from reacting to disputes after the fact to ensuring that the system remains resilient regardless of which cable breaks, where, or why.

Primary cable regulators in each state should condition landing rights on the owner's participation in a resilience pool: a shared fund to which all licensed operators contribute annually and from which resources are reallocated on a regular, predictable cycle. Unlike a traditional insurance fund that pays out only after a loss, this pool would distribute funds each year based on operators' performance against a set of measurable resilience benchmarks. These benchmarks should include, at a minimum, the degree of investment in retrofitting cables to withstand natural hazards and to incorporate state-of-the-art technology, the extent to which redundancy has been added to the system through new routes or additional capacity, and the

[13] Exec. Order No. 10530, 3 C.F.R. 189 (1954–1958 Comp.).
[14] RICHARD SALGADO, UNDERSEA CABLES, HYPERSCALERS, AND NATIONAL SECURITY 7–8 (2023), https://www.hoover.org/sites/default/files/research/docs/Salgado_finalfile_WebReadyPDF.pdf [https://perma.cc/39FU-3C5D].
[15] National Security Division, *Team Telecom*, U.S. DEP'T OF JUST. NAT'L SEC. DIV.: OUR WORK (Sep. 20, 2023), https://www.justice.gov/nsd/team-telecom [https://perma.cc/U887-CSXS].
[16] SALGADO, *supra* note 14, at 9–10.

willingness of operators to share timely information about breaks, near-misses, and ship activity that threatens cable integrity with states.

Operators that demonstrate sustained contributions to system-wide resilience receive rebates or reduced forward-looking contributions. Those that fail to meet standards see their obligations rise. The pool therefore serves two purposes at once: it acts as a reserve for rapid repair, and it provides an incentive mechanism that channels private capital into prevention, redundancy, and transparency. Embedding this obligation in the licensing process guarantees universal participation. It also allows for regular recalibration of standards and formulas. Finally, it avoids the inertia that has long plagued statutory and treaty-based approaches.

By shifting accountability into a pooled regime, this approach reduces the counterproductive fixation on cable-by-cable assessments that now dominate regulatory and legal processes. Today, every break or license application is scrutinized in isolation, producing duplicative investigations, inconsistent standards, and delays that compound system fragility. A resilience pool instead directs legal, economic, and policy attention to the health of the network as a whole. Performance is judged across the aggregate system—how much redundancy exists in critical corridors, how quickly capacity is restored after outages, how well information flows among operators and states—rather than through piecemeal adjudication of individual incidents. This systemic orientation encourages operators to think beyond their own assets, rewards investments that benefit the wider ecosystem, and equips regulators with a more holistic picture of resilience than could ever emerge from one-off, cable-specific proceedings.

Licensing is the proper legal hook because it is universal, adjustable, and transaction-proximate.[17] Every international cable touches at least one coastal regulator at the landing stage. License conditions can be tailored to route, seabed conditions, and local risks; they can also be revised as technologies, threat vectors, and traffic patterns evolve. By embedding resilience obligations in this existing and iterative process, states can upend today's diffuse accountability without waiting on legislatures or international conferences.

The resilience pool addresses the core market failure by requiring cable owners to collectively bear the costs of system-wide risks. Instead of treating resilience as a public good that is chronically underprovided, the pool makes it a priced obligation through an annual fund capitalized by all licensed operators. Each operator's contribution would be calibrated to its risk profile: companies operating routes through high-hazard zones (such as seismic trenches, heavy-fishing corridors, or anchor-dense approaches) or with poor performance histories contribute more, while those that exceed resilience standards contribute less. This structure transforms resilience investments—from stronger armoring to smarter routing to continuous monitoring—from voluntary, charitable outlays into rational, financially rewarded business decisions.

[17] *See* UPTAL KUMAR RAHA & RAJU K. D., SUBMARINE CABLES PROTECTION AND REGULATIONS: A COMPARATIVE ANALYSIS AND MODEL FRAMEWORK 159–171 (2021) (describing licensing as part of the proposed model law for submarine cables).

The pool should be administered by a neutral private entity that is chartered specifically for this purpose and formally recognized by each state's cable regulator. Its governing board must be carefully designed to reflect the range of stakeholders whose interests are bound up in the resilience of the undersea cable system. Public authorities responsible for maritime safety, telecommunications, and national security should hold non-voting seats. Their presence would enable regulators to remain fully informed and allow them to provide guidance, but their lack of voting power would mitigate against political considerations overwhelming the technical and operational focus of the pool. Cable owners should hold voting seats, with the weight of their vote proportionate to their assessed risk exposure. This arrangement increases the odds that those who bear the greatest responsibility for resilience also carry the greatest responsibility for decision-making, while conflict-of-interest rules prevent dominant players from shaping standards to their advantage. Finally, an independent technical committee should be established to develop, update, and refine the standards for "responsible cable management." This approach ties operational requirements to the latest engineering, monitoring, and security practices, rather than to the short-term interests of any one group. The administrator, working under this board structure, must have clear authority to audit operator compliance, commission forensic reviews after incidents, and publish anonymized benchmarks that allow both regulators and industry to track system-wide performance over time.

The administrator would also be responsible for setting and regularly updating a clear set of best-practice standards applicable to each cable operator. These standards should undergo a thorough review on a fixed schedule—such as once a year—with the flexibility to issue interim updates whenever new threats emerge. At a minimum, the standards would address four areas. First, engineering: requirements for how cables are armored and buried depending on depth and local conditions, specifications for repeaters and sensors that allow rapid fault detection, and benchmarks for ensuring sufficient redundancy along critical routes. Second, monitoring: expectations for continuous tracking of vessel activity near cables, the use of sensors to detect anomalies along the line, and surveillance—whether by drones, unmanned vessels, or other means—around vulnerable landing points. Third, repair readiness: minimum stockpiles of spare parts, pre-positioned equipment along likely fault zones, access to repair ships on short notice, and regular drills to practice restoring service. Fourth, landing-site protection: physical security for facilities, backup power supplies, and safeguards against hazards such as flooding or fire. Each of these standards would include measurable benchmarks—for example, how quickly faults are detected and repaired, what percentage of the route meets burial depth requirements, and how frequently inspections are carried out—so that performance can be monitored and compared across operators.

Each operator's annual contribution to the pool would be calculated using a transparent formula that takes three factors into account. The first is a route risk score, which reflects the hazards along a given cable path, such as seismic activity, heavy fishing, or dense shipping traffic. The second is an operator performance score, which measures how often that company's cables have broken relative to the risks they face, how quickly they were repaired, and how well the company has complied with past audits. The third is a practice adoption score, which evaluates how fully and how quickly the operator has adopted the most recent resilience standards. Together, these scores determine whether an operator pays more into the pool or less.

Companies that consistently perform well receive rebates or see their future contributions reduced, while companies that lag behind face higher costs. If poor performance continues, operators could face stricter consequences, such as probationary licenses or requirements to post financial bonds. By structuring contributions this way, the system creates a sliding scale that rewards good practices, penalizes negligence, and ultimately makes resilience a source of competitive advantage.

The pool's resources would be deployed with the system's longevity and utility in mind—covering emergency repairs and building long-term resilience into the system. When a break occurs and meets predefined thresholds, funds could be drawn immediately to pay for restoration, ensuring that response times are not slowed by disputes over responsibility. Beyond emergencies, the pool can support readiness by maintaining spare parts in depots near vulnerable corridors, underwriting access to repair ships so they are available on short notice, and financing joint training exercises that keep crews prepared. A portion of the funds should also be devoted to research and development, with an emphasis on technologies that improve fault detection, enhance cable durability, and enable more efficient seabed inspections. Finally, pooled resources can sustain shared information systems that track vessel traffic and other maritime risks in real time. To safeguard the fund itself, a catastrophe backstop—such as parametric reinsurance or a catastrophe bond—would activate in the rare event of a large-scale outage affecting multiple cables, ensuring that one disaster does not exhaust the collective reserve.

License conditions should also impose strict timelines for reporting incidents, so that information flows quickly and consistently across the system. Within 24 hours of detecting an anomaly, operators would be required to issue a preliminary notice, ensuring that regulators and the pool administrator are alerted at the earliest stage. A more detailed technical report would follow within seven days, and a comprehensive root-cause analysis would be submitted within sixty days. Each report would use a standardized set of categories—such as natural event, fishing gear interaction, anchor drag, intentional interference, or unknown cause—to ensure comparability across operators and incidents. To verify the findings, operators would be obliged to share sensor data and vessel-tracking information (AIS), subject to appropriate privacy and security protections. Where the evidence points to a third party, such as a vessel responsible for the damage, the pool rather than the individual operator would take the lead in pursuing recovery of costs. This subrogation mechanism not only relieves operators of expensive and uncertain litigation but also strengthens the likelihood that responsible parties are held to account.

Participation in the pool would also come with a safe-harbor regime designed to encourage transparency. Operators that promptly share telemetry, incident reports, and other required data would receive legal protections for good-faith disclosures, reducing the risk that their cooperation could later be used against them. To further build trust, all shared data would be shielded from public release and disclosed only in anonymized or aggregated form, ensuring that sensitive operational information cannot be exploited by competitors or adversaries. By contrast, operators that withhold information or delay disclosures without justification would face tangible consequences, including higher contributions to the pool and potential threats to their

licensing status. In this way, the system rewards openness while penalizing secrecy, aligning private incentives with the collective need for timely and accurate information.

Enforcement ultimately rests on the one tool regulators cannot delegate: control over landing rights. An operator that fails to meet its obligations—whether by neglecting to pay assessments, ignoring standards, or withholding required disclosures—should face escalating consequences, culminating in the suspension or denial of licenses after due process. In cases of persistent or egregious non-compliance, regulators may also require financial guarantees such as performance bonds or letters of credit sized to the operator's risk profile. These instruments ensure that funds are available for remediation even if the operator defaults, closing off the possibility that bad actors externalize costs to the system as a whole.

Cross-border alignment is achievable through mutual recognition at the license layer. Because most systems land in multiple jurisdictions, regulators should recognize a single operator compliance dossier and a common standards set, while preserving jurisdiction-specific add-ons for local hazards. Contributions can be prorated by route segment and landing jurisdiction, with credits portable across systems. This reduces duplicative audits while maintaining national prerogatives at the shoreline.

Revisiting the opening hypothetical helps to illustrate the value of this shift. A fishing vessel from Country A, crewed by nationals of Country B, severs a cable owned by a company in Country C, with one end landing in Country D. Under the current system, regulators and courts would immediately be drawn into a tangle of questions about flags, ownership, and jurisdiction before any repair could even begin. The pooled model changes the sequence entirely. Because operators have already internalized responsibility through licensing and annual contributions, the pool can release funds the moment a break is confirmed, ensuring that repair crews mobilize without waiting for fault to be assigned. The telemetry and reporting requirements still generate a shared evidentiary record, but that information is used to improve system-wide resilience and, where possible, to recover costs from a clearly culpable third party. The primary focus of the pool is not to litigate every incident but to guarantee continuity of service and channel resources toward prevention and rapid restoration. In this way, disputes over who is to blame occur after cables are back online, while the broader system remains resilient throughout.

The strength of this reconception lies in its refusal to replicate the flaws of the current system. Today, resilience is treated as the byproduct of resolving each cable dispute—an approach that consumes resources in litigation, produces inconsistent outcomes, and leaves the global network vulnerable while lawyers and regulators argue over flags, ownership, and jurisdiction. The pooled model reverses that sequence. It ensures that resilience is the first priority: cables are repaired immediately, redundancy is built out in advance, and system-wide performance steadily improves through predictable incentives. Disputes over who caused a particular break or who should ultimately bear the cost do not disappear, but they are moved to the background, addressed only after continuity of service is restored. In short, the focus of law and policy shifts from allocating blame in individual cases to safeguarding the health of the entire network. That inversion—system first, disputes second—is the only way to keep pace with the demands of an infrastructure on which economies, democracies, and defense now depend.

APPENDIX C

JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOL. 13 • NO. 1 • 2021 – 2022

POLICY PROPOSALS FOR THE UNITED STATES TO PROTECT THE UNDERSEA CABLE SYSTEM

Kevin Frazier

The protection of the undersea cable system, which carries the vast majority of the world's Internet traffic, requires a new policy approach from the United States government. Old vulnerabilities and new threats have placed this critical piece of international infrastructure under increased threat of disruption and sabotage. Old vulnerabilities include the inherent difficulties associated with defending cables that lay along the open seafloor across international waters and the fragility of the cables themselves--often no larger than a garden hose. New threats come from climate change and changes in geopolitics. For example, Russia, among other nations, has made investments in offensive military equipment tailored to breaking undersea cables.

Though disruptions to Internet traffic through the undersea cable system can be diverted to satellites, that alternative comes with significant financial and temporal costs. Therefore, proactive policies to prevent cable breaks should receive substantial attention from political leaders. The weeks and millions of dollars required to repair broken cables further justify the prioritization of proactive policies to reduce the frequency of breaks.

This article explores why current international and domestic laws and policies meant to protect undersea cables fall short of what is needed to ensure the longevity and security of the undersea cable system. After an analysis of these various laws and policies, the article offers a series of steps the Biden Administration can take to improve the resilience of the undersea cable system, at least the parts of it connected to the United States.

These steps make theoretical sense and have received support from policy leaders on this topic--actually taking the steps, though, will require significant political capital. The majority of the undersea cable system is owned and operated by private stakeholders. The protection of the system necessitates extensive collaboration between private and public stakeholders. Because collaboration takes time and trust, this article comes at a critical moment -- it can help direct political energy toward this time-sensitive endeavor.

CONTENTS

I. Introduction – A Vulnerable, Critical System

Picture this hypothetical: in the dark cloud of night, several Russian submariners prep for a world-changing mission. Covered by an even darker sea, the submarines sail west to the coast of California; more specifically, the submarines target a small slice of the coast—the approximate 200 miles between Morro Bay and Redondo Beach in which seventeen different undersea cables lay unprotected on the ocean floor.[1] After decades of investment in its Pacific Fleet,[2] the Russian government is ready to reap a return in the form of disrupting the Internet.

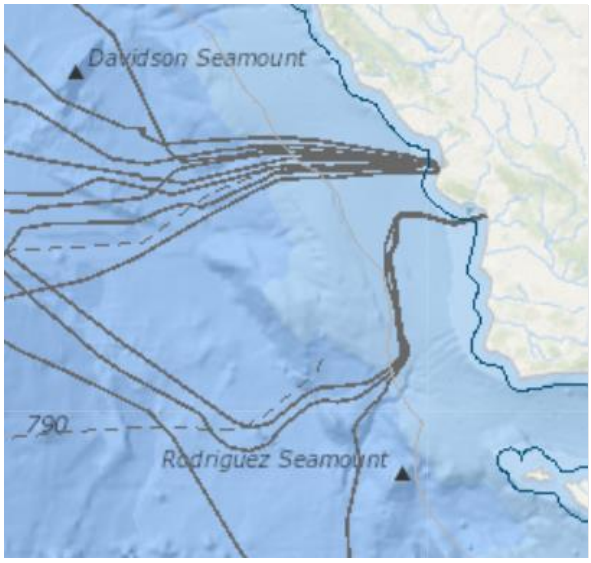


FIGURE 1: Depiction of the undersea cables off the coast of California.[3]

Once in place, the submarines begin their operation. Designed to perform technical work on the ocean floor, these machines are equipped for the task at

[1] TELEGEOGRAPHY (visual count of cables taken on Jan. 22, 2021), https://www.submarinecablemap.com/multiselect/landing-point?ids=morro-bay-ca-united-states,redondo-beach-ca-united-states,hawaii-kai-hi-united-states,lurin-peru [https://perma.cc/9Q38-FMJV].

[2] Peter Suciu, *Russia's Pacific Fleet Is Getting Stronger. Here's Why That Matters*, NAT'L INT. (June 2, 2020), https://nationalinterest.org/blog/buzz/russias-pacific-fleet-getting-stronger-heres-why-matters-159506 [perma.cc/9HCC-QSDM].

[3] *Marine Cadastre National Viewer,* OFF. COASTAL MGMT. (Jan. 22, 2021), https://marinecadastre.gov/nationalviewer/.

hand:[4] cutting the undersea cables—not that it is especially hard given that the cables are comparable in size to garden hoses.[5]

The small breaks in each of the cables amount to large disruptions to Internet access at both ends of the cables—the contiguous United States, where the cables launch, and the respective end destinations of the cables, including Hawaii, Japan, the Philippines, and Peru.[6] Internet service continues in each of these places but at much slower speeds. The undersea cable system is fairly redundant[7]—meaning that multiple cables often land at a single destination to prevent a single cable break from causing too much disruption.[8] However, a geographically-specific attack such as this one would force more Internet traffic to travel through satellites because the redundancy of the system would become a bug, rather than a feature. The high number of cables in close proximity would allow for a few submarines to knock out many cables. The resulting shift in traffic would result in lower quality, less reliability, less security, and more expensive Internet service.[9] Undersea cables, made up of fiber optic cores, "transfer data five times faster than satellites [and] do so at a vastly lower cost," according to Rishi Sunak, British Parliamentarian and author of a report on undersea cables.[10]

With Americans tweeting, albeit with less speed, about their sluggish Internet, the *USNS Zeus*, the U.S. Navy's lone cable repair ship,[11] mobilizes . . .

---

[4] Magnus Nordenman, *Russian Subs Are Sniffing Around Transatlantic Cables. Here's What to Do About It*, DEF. ONE (Jan. 17, 2018), https://www.defenseone.com/ideas/2018/01/russian-subs-are-sniffing-around-transatlantic-cables-heres-what-do-about-it/145241/.

[5] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, STRATEGIC IMPORTANCE OF, AND DEPENDENCE ON, UNDERSEA CABLES 1 (Nov. 2019), https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf [hereinafter CCDCOE].

[6] TELEGEOGRAPHY, *supra* note 1.

[7] *See* Garrett Hinck, *Evaluating the Russian Threat to Undersea Cables*, LAWFARE BLOG (Mar. 5, 2018, 7:00 AM), https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables [https://perma.cc/63R3-7XRQ] (outlining the redundancy of the undersea cable network by pointing out that "[c]utting the United States off from the rest of the world would require severing a large number of cables: at least 18 in the North Atlantic alone . . .").

[8] *Id.*

[9] THE COMMUNICATIONS SEC., RELIABILITY AND INTEROPERABILITY COUNCIL IV, WORKING GROUP 8 SUBMARINE CABLE ROUTING AND LANDING 1 (Dec. 2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf [https://perma.cc/39ZA-AABG] [hereinafter WORKING GROUP REPORT].

[10] RISHI SUNAK, UNDERSEA CABLES: INDISPENSABLE, INSECURE 13 (Dec. 1, 2017), https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

[11] *See* Hinck, *supra* note 7 (noting that "Congress authorized $250 million for a new ship that can lay and repair cables" in the U.S. defense authorization bill for fiscal 2018).

from Norfolk, Virginia . . . to respond to the threat in California.[12] Public and private actors demand a more expedient solution but receive an unsatisfactory response because the Navy has not outlined a plan for defending undersea cables.[13] Ultimately, the United States Federal Government calls on the International Cable Protection Committee (ICPC) for assistance. The ICPC, whose 170 members account for ownership of 97 percent of the world's undersea telecom cables,[14] coordinates a fleet of undersea cable repair ships. After several weeks and more than $17 million in repair costs,[15] the cables are restored.

This hypothetical is not far from reality. In 2008, an accidental cable break in the Mediterranean Sea diminished the reliability and quality of the Internet to such an extent that the United States military had to scale back its drone operations in the Middle East by an order of magnitude.[16] Similarly, when a cable connected to Vietnam failed in 2017, Internet customers in Ho Chi Minh briefly lost connectivity.[17] Intentional breaks of cables have also wreaked havoc on some nation states while advancing the aims of others and affiliated non-state actors.[18] As flagged by the think tank Chatham House and reported by the BBC, Ukrainian telecom providers noticed disruptions to an essential Internet exchange point as well as to cable connections in the midst of Russia's military action in the Crimean Peninsula in 2014.[19]

The under-discussed importance and vulnerability of the undersea cable system merit increased attention from, and action by United States policymakers. Society's increased reliance on the Internet justifies addressing the vulnerabilities of the system.[20] Additionally, absent action in the short-run, other activities in the

---

[12] *See generally* Voyage information of *USNS Zeus*, MARINETRAFFIC, https://www.marinetraffic.com/en/ais/details/ships/shipid:5430967/mmsi:367212000/imo:7932408/vessel:ZEUS#:~:text=ZEUS%20(IMO%3A%207932408)%20is,her%20width%20is%2022.25%20meters (documenting the various locations of the USNS Zeus, some of which are on or beyond the eastern coast of the United States) (last visited Nov. 7, 2021).

[13] Hinck, *supra* note 7.

[14] INT'L CABLE PROT. COMM., https://www.iscpc.org/ [hereinafter ICPC] (last visited Nov. 7, 2021).

[15] CCDCOE, *supra* note 5, at 3 (noting that it may take "several weeks and cost in excess of one million USD for a repair to be completed").

[16] Hinck, *supra* note 7.

[17] *Id.*

[18] *Id.*

[19] Chris Baraniuk, *Could Russian submarines cut off the internet?*, BBC (Oct. 26, 2015), https://www.bbc.com/news/technology-34639148 [https://perma.cc/25U6-R6HX] (quoting a representative of Chatham House as saying, "[Russia] can interfere with internet infrastructure in order to gain [complete] control of [the information available in] specific regions").

[20] WORKING GROUP REPORT, *supra* note 9, at 1.

sea will make future efforts to remedy the system even harder; increased exploration and exploitation of the seabed, for instance, is bringing new stakeholders into the proverbial arena and threatening to crowd out the interests of undersea cable operators.[21]

This paper contains six sections: a discussion of the importance of the undersea cable system to the Internet, an overview of the sources and severity of risks to that system, an assessment of the adequacy of the various legal frameworks and industry standards related to the system, a review of actions by other public and private actors to protect the system, an examination of the shortcomings of United States law and policy related to the system, and a proposal for policy responses by the United States.

Several issues are outside the scope of this paper. The impact of the undersea cable system on marine life and ecosystems will go uncovered. An authoritative report produced, in part, by the ICPC reports that the "laying of [undersea cables] on the surface of the ocean floor has a minor if not negligible one-off impact."[22] Nevertheless, some of the solutions discussed in Section VII may benefit marine life and ecosystems. Those secondary benefits will be left to others to fully examine.[23] This paper will also not provide a thorough examination of the issues related to cybersecurity and espionage associated with the undersea cable system. The decision to avoid these topics is based on the difficulty of eavesdropping via undersea cables and the ease of other means to accomplish the same objective.[24]

This paper instead is focused on raising awareness around the vulnerability of the undersea cable system during a time, in the midst of the COVID-19 pandemic, when Internet access is more important than ever.[25]

---

[21] *Id.* at 3.

[22] CARTER ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD 37 (UNEP-WCMC Biodiversity Series No. 31 2009).

[23] *See, e.g.*, Kingsley Ekwere, *Submarine Cables and the Marine Environment: Enhancing Sustainable and Harmonious Interactions*, 2016 CHINA OCEANS L. REV. 154, 161 (2016).

[24] *See, e.g.*, Richard Chirgwin, *Spies need superpowers to tap undersea cables*, THE REGISTER (Sept. 18, 2014), https://www.theregister.com/2014/09/18/spies_arent_superheroes/ [https://perma.cc/N9QQ-FUFW] (discussing the dangerous and resource intensive steps required to safely and effectively tap an undersea cable, noting that few nations possess the submarines requisite for such an activity, and pointing out three far easier means to get the same sort of information).

[25] Jessica Poiner, *In the midst of coronavirus, connectivity matters more than ever*, OHIO GADFLY DAILY (July 23, 2020), https://fordhaminstitute.org/ohio/commentary/midst-coronavirus-connectivity-matters-more-ever [https://perma.cc/6JEZ-4B99].

Furthermore, this paper aims to motivate action from Federal Government stakeholders in the wake of the transition to a new presidential administration; this transition presents an opportunity to reassess the current United States legal and policy approaches to the protection of the undersea cable system.

The paper will reveal the following conclusions: first, the protection of the undersea cable system is essential to a functioning Internet and, therefore, the economy, culture, and governance; second, intentional attacks by state and non-state actors and unintentional breaks by commercial actors pose the two greatest threats to the system; third, international law inadequately addresses those threats; fourth, United States domestic law also insufficiently addresses those threats; and, fifth, the United States Federal Government can most effectively and efficiently reduce the likelihood of those threats occurring and the severity of damage those threats could cause by partnering with the owners of the cables themselves to implement policy solutions.

II. The Undersea Cable System is Essential to a Fast and Reliable Internet

Undersea cables are foundational to a safe, reliable, and global Internet. Upwards of 97 percent of all Internet traffic travels on undersea cables.[26] "Submarine cables," as reported by The Working Group of the Communications Security, Reliability, and Interoperability Council, "provide the principle domestic connectivity between the contiguous United States" and its offshore states and territories (see Figure 2).[27] As of 2014, Internet cables carried more than 95 percent of United States Internet traffic, a percentage that is almost assuredly higher as of this writing.[28] Most of these cables have a series of fiber optic cables at their core; these cables are hair-thin strands of glass that allow for data to travel as wavelengths of light at speeds of approximately 180,000 miles per second.[29]

[26] CCDCOE, *supra* note 5, at 1.
[27] WORKING GROUP REPORT, *supra* note 9, at 1.
[28] *Id*.
[29] SUNAK, *supra* note 10, at 14.

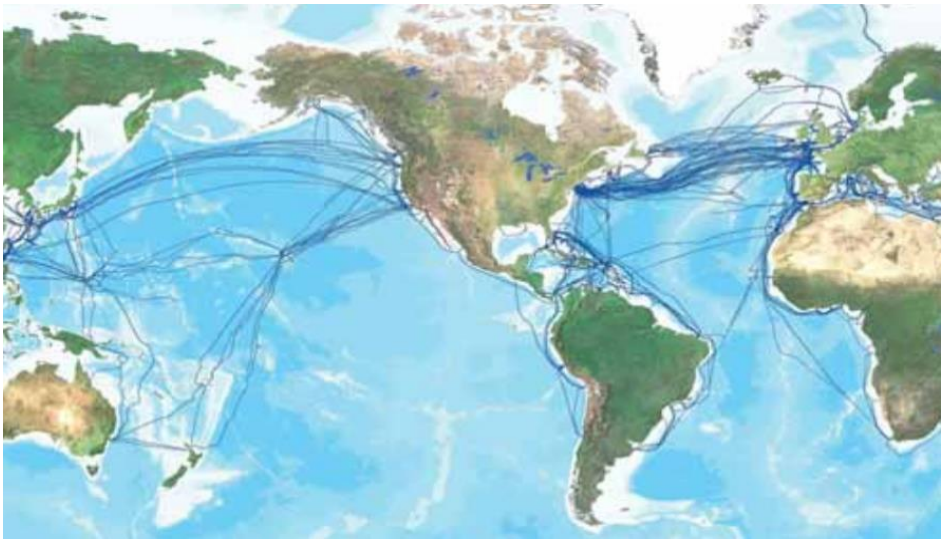


FIGURE 2: Undersea communications cables as of 2009.[30]

The private and public sectors rely almost exclusively on privately-owned cables to carry their Internet traffic. The importance of these cables to private and public interests qualifies them as "critical infrastructure" according to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).[31] Regular or persistent disruption to these cables could undermine modern society's ability to function.[32] The destruction of or disruption to an undersea cable may cut an entire area off from the Internet. Whether that area remains connected depends on the number of redundant cables and the existence of alternative routes for the Internet traffic, such as satellites.[33] What's more, as the number of people with Internet access increases around the world, the integrity of the cables will grow in importance due to the increase in the amount of data that will travel through the cable system.[34]

Despite the fact that undersea cables "carry the vast majority of civilian and military U.S. Government traffic, [as of 2014] the U.S. Government does not own and operate its own submarine cables."[35] The Federal Government has laid some of its own cables;[36] nevertheless, a Harvard report revealed that the agency

[30] CARTER ET AL., *supra* note 22, at 11.
[31] CCDCOE, *supra* note 5, at 1.
[32] *Id.* (comparing the cables to the "central nervous system" of the global Internet).
[33] *See id*. at 2.
[34] *Id.*
[35] WORKING GROUP REPORT, *supra* note 9, at 1.
[36] Hinck, *supra* note 7 (stating that the Pentagon has "publicly acknowledged [laying its own] cables connecting Miami to the naval base at Guantanamo Bay").

responsible for the Department of Defense's Internet networks depends on privately-owned cables for 95 percent of their strategic communications—indicating continued government reliance on private cables to carry even the most sensitive data.[37] This reliance on the undersea cable system means that "[d]amage to [the system] can pose grave risks to U.S. national security and the U.S. economy."[38] The number of cables running along the United States coastline further increases the importance of the integrity of the system to the United States military. Within the territorial sea, exclusive economic zone (EEZ), and outer continental shelf (OCS) of the United States there are at least 55 in-service submarine cable systems and at least a dozen have been proposed or are currently under construction.[39] These cables represent potential targets for foreign states, and non-state actors such as terrorist organizations.[40]

Private-sector entities likewise rely on the undersea cable system for fast, reliable Internet. "[A]n estimated $10 trillion in financial transfers and vast amounts of data pass through the seabed routes" on a daily basis.[41] The importance of the Internet to the economy has drawn the capital of some of the world's largest and most powerful companies. Though telecom carriers previously owned the majority of cables, their share of the system has decreased because of the entrance of Internet content providers, such as Facebook and Google, into the cable-laying business.[42]

Absent the undersea cable system, the public would experience slower Internet speeds.[43] Internet traffic routed through satellites is lower in quality, less reliable, less secure, and more expensive.[44] Consider that modern-day cables are engineered to the same "five-nines" standard as nuclear weapons and space shuttles—a standard which means they are reliable 99.999 percent of the time.[45] For all of its benefits, some aspects of the undersea cable system can raise the consternation of the public. Residents of a small town on the Oregon coast, for example, have decried Facebook's placement of a cable landing station ("CLS")

---

[37] *Id.*
[38] WORKING GROUP REPORT, *supra* note 9, at 2.
[39] *Id*. at 1.
[40] *See generally id.* at 2 (discussing how critical infrastructure is for both civilian and military purposes in the United States).
[41] Tim Johnson McClatchy, *Undersea Cables: Too Valuable to Leave Vulnerable?*, GOVTECH (Dec. 12, 2017), https://www.govtech.com/network/Undersea-Cables-Too-Valuable-to-Leave-Vulnerable.html [https://perma.cc/A3AU-7S4B].
[42] CCDCOE, *supra* note 5, at 1.
[43] WORKING GROUP REPORT, *supra* note 9, at 1.
[44] *Id*.
[45] SUNAK, *supra* note 10, at 15.

in the community.[46] Notwithstanding issues related to the land-based infrastructure of the undersea cable system, the public experiences tremendous benefits from the system.

III. Two Types of Threats Must be Addressed to Secure the Undersea Cable System

The physical characteristics of the undersea cables make them susceptible to intentional and unintentional disruption. Cables that connect continents or lands divided by open water rest on the ocean floor.[47] The average diameter of these cables is comparable to that of a garden hose.[48] The planned commercial lifespan of the cables is 25 years, though they often get used for longer periods of time.[49] Closer to the coast, the cables often have external steel wire rods for protection and, in some cases, are placed up to two meters beneath the surface.[50] CLS are also susceptible to natural and human-based threats, though threats to these sites will not be discussed here.

Most experts regard the breakage rate of undersea cables as "rare" given the scale of the system;[51] there are about 100 undersea cables breaks per year.[52] Though "rare," the frequency of breaks incentivizes cable owners as well as those reliant on cables to lay additional, seemingly redundant cables to increase the resiliency of the cable system.[53]

The high costs of repairs and difficult logistics of those repairs also incentivizes cable system owners to protect cables and lay extra ones. Timely repair of cables necessitates "ready and unfettered access for cable ships and equipment to the ocean surface, water column, and seabed around a submarine

---

[46] Nigel Jaquiss, *Mark Zuckerberg Is Despoiling a Tiny Coastal Village and Oregon's Natural Treasures. The State Invited Him*., WILLAMETTE WEEK (Aug. 19, 2020), https://www.wweek.com/news/2020/08/19/mark-zuckerberg-is-despoiling-a-tiny-coastal-village-and-oregons-natural-treasures-the-state-invited-him/ [https://perma.cc/G57P-Y3KY].
[47] CCDCOE, *supra* note 5, at 1.
[48] *Id.*
[49] WORKING GROUP REPORT, *supra* note 9, at 1.
[50] *See id*.
[51] *Id*. (regarding the frequency of damage to submarine cables as "rare"); *See also* McClatchy, *supra* note 41 (estimating an average of 200 failures along cable routes per year along approximately 650,000 miles of active international commercial cables).
[52] CCDCOE, *supra* note 5, at 2.
[53] *See id*.; *see also* Hinck, *supra* note 7 (outlining the redundancy of the undersea cable network by pointing out that "[c]utting the United States off from the rest of the world would require severing a large number of cables: at least 18 in the North Atlantic alone . . .").

cable."[54] Obtaining such access requires extensive coordination and cooperation mechanisms, including, but not limited to, "cable spacing and crossing standards, cable awareness programs and outreach, coordinating with other users of marine and coastal areas, and marine special planning."[55] Cable ships need a lot of room in order to complete their repairs.[56] Objects such as "oil platforms, turbine towers, [and] submerged structures" all frustrate the timely repair of cables.[57]

FIGURE 3: "Diver Checking Underwater Protection of Cable"[58]

Unintentional events in waters shallower than 200 meters account for the majority of cable breaks.[59] Unintentional breaks include those caused by natural forces as well as some human-caused breaks.[60] Natural events, such as earthquakes along the Pacific Rim, regularly break undersea cables.[61] The

[54] WORKING GROUP REPORT, *supra* note 9, at 3.
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Driver Checking Underwater Protection of Cable* (photograph), *in* The Official CTBTO Photostream, FLICKR (Aug. 13, 2009), https://search.creati9vecommons.org/photos/b9d8b72a-3cb5-4405-a55c-b0c6a047ba17.
[59] CARTER ET AL., *supra* note 22, at 39.
[60] *Id.*
[61] *See, e.g.*, Winston Qiu, *Submarine Cables Cut by Taiwan Earthquake and Typhoon Morakot*, SUBMARINE CABLE NETWORKS (Mar. 19, 2011), https://www.submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006.

unintentional byproducts of human actions, such as commercial fishing activities including anchoring and fishing, are the most frequent cause of undersea cable breaks.[62] For example, in 2012, a ship off the coast of Mombasa accidentally dropped its anchor on the East African Marine System (TEAMS), a cable laid by the Government of Kenya to increase its connectivity to the rest of the Internet.[63] As a result, six African nations saw the normal flow of Internet traffic drop by 20 percent; the repair time was estimated to be three weeks, while costs were forecasted to reach $500 million.[64] This sort of damage and disruption, though, is not typical of the regular breaks that occur from unintentional breaks.[65]

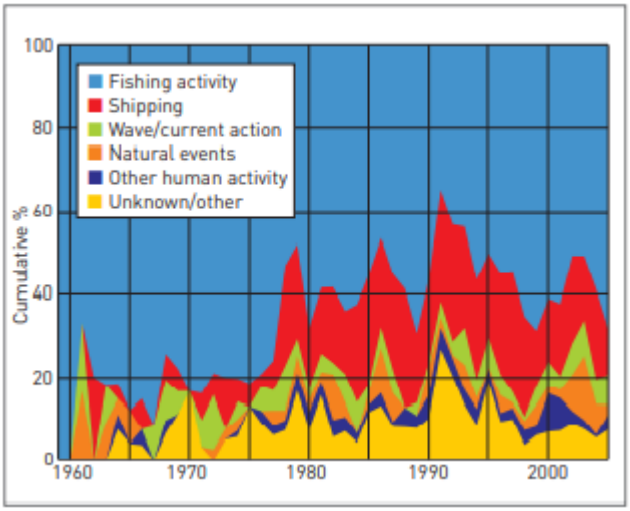


FIGURE 4: Types of cable breaks recorded between 1959 and 2000.[66]

Given that commercial activity causes the majority of cable breaks, any meaningful effort — be it legal or extralegal — to protect the undersea cable system must address these events. As the TEAMS example makes clear, the randomness of these commercially-induced breaks does not make for a straightforward policy response to reduce their frequency. The rarity of natural

[62] *See* CCDCOE, *supra* note 5, at 2.
[63] Curt Hopkins, *Ship's anchor cuts Internet access to six East African countries*, CHRISTIAN SCI. MONITOR (Feb. 29, 2012), https://www.csmonitor.com/World/Africa/2012/0229/Ship-s-anchor-cuts-Internet-access-to-six-East-African-countries.
[64] *See id*.
[65] WORKING GROUP REPORT, *supra* note 9, at 2; CCDCOE, *supra* note 5, at 2.
[66] Matthew P. Wood & Lionel Carter, *Whale Entanglements with Submarine Telecommunication Cables*, 33 IEEE J. OCEANIC ENG'G 445, 446, fig.1 (2008).

events causing breaks means that these events ought not to significantly influence policy decisions.[67]

A policy designed to ensure the integrity of the undersea cable system should also consider the threats posed by undersea cable system attackers. These actors have clear ample reason to target the undersea cable system as a means to injure an adversary. By way of example, an adversary who intentionally broke specific cables along the United States coast could "cause a significant network disruption that could hamper a United States military response in the opening hours of a major war," at least according to a former deputy director of the National Security Agency.[68] It appears as though nations such as Russia are increasingly investing in the resources necessary to cause such breaks.[69]

Non-state actors may also intentionally interfere with undersea cables for non-political reasons. The Vietnamese military responded to one such incident when local officials permitted fishermen in town to harvest copper from old cables off the Vietnam coast.[70] When doing so, the fishermen attempted to take resources from newer cables as well.[71] The resulting damage to the undersea cable system caused 82 percent of the Internet traffic to drop in the short run and, in the long run, cost US $5.8 million to restore to normal service.[72] Whatever motive instigates the intentional breaking of a cable, these deliberate and geographically-specific attacks can significantly disrupt Internet service.

Intentional threats, then, have the potential to be more disruptive than the more-frequent unintentional, commercial threats. That is precisely why policies focused on ensuring the integrity of the system should prioritize responding to intentional attacks and unintentional, commercial threats—the former is more disruptive, and the latter is more common.

---

[67] Not only are unintentional, natural events causing breaks infrequent, they are also more predictable. For instance, a nation may identify that a typhoon is coming and, to the extent possible, ready its private and government cable repair ships. Intentional breaks are likewise infrequent, but their unpredictability renders them a greater threat to the integrity of the undersea cable system because no such advanced preparation can take place.

[68] Hinck, *supra* note 7.

[69] *Id.*

[70] Mick P. Green & Douglass R. Burnett, *Security of International Submarine Cable Infrastructure: Time to Rethink?*, *in* LEGAL CHALLENGES IN MARITIME SECURITY 557, 561–62 (Myron H. Nordquist et al. eds., 2008).

[71] *Id.* at 562.

[72] MICHAEL SECHRIST, CYBERSPACE IN DEEP WATER: PROTECTING UNDERSEA COMMUNICATION CABLES BY CREATING AN INTERNATIONAL PUBLIC-PRIVATE PARTNERSHIP, BELFER CTR. 123 (Mar. 23, 2010), https://www.belfercenter.org/sites/default/files/legacy/files/PAE_final_draft_-_043010.pdf.

IV. Current Legal and Extralegal Frameworks do not Sufficiently Address the Threats to the Undersea Cable System

The international and national laws pertaining to the undersea cable system are outdated and insufficient.[73] Industry standards meant to coordinate the actions of the private cable owners also fall short.[74] These insufficiencies are not because of a lack of awareness surrounding the importance of the undersea cable system. Going as far back as 1884, undersea cables have received special protection under international laws.[75] Since then, international law pertaining to the cables has not substantially progressed. Some nations have opted to fill in the blanks left by the international regime; these efforts, though, have limited efficacy so long as the international regime fails to empower nations to take proactive acts to protect their cables, especially in international waters. This paper will not perform a full exploration of these laws, customs, and standards. Instead, this part will focus on the law as it is understood and applied today, particularly from the perspective of the United States.

Which laws, customs, and standards apply to the undersea cable system depends on the distance of the cable from the relevant coastal state.[76] Intuitively, as the distance from the coastal state increases, the legal rights of that coastal state diminish.

The first legal zone, the one most proximate to the coastal state, is the territorial sea.[77] According to the United Nations Convention on the Law of the Sea (UNCLOS), "[t]he sovereignty of a coastal State extends . . . to an adjacent belt of sea," known as the territorial sea.[78] Every State has the right to exercise such sovereignty in the seas within 12 nautical miles of their coast.[79]

---

[73] *See* UNCLOS DEBATE, *U.S. underseas cable industry needs UNCLOS protection*, https://www.unclosdebate.org/argument/708/us-underseas-cable-industry-needs-unclos-protection (last visited Sept. 15, 2021).
[74] WORKING GROUP REPORT, *supra* note 9, at 45–46.
[75] Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884 [hereinafter "1884 Convention"]; CCDCOE, *supra* note 5, at 4 (outlining some provisions of the Convention for the Protection of Submarine Telegraph Cables).
[76] *See generally* United Nations Convention on the Law of the Sea art. 2, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter "UNCLOS"] (establishing a legal framework for all marine and maritime activities).
[77] *Id.* at art. 2, ¶ 2.
[78] *Id.*
[79] *Id.* at art. 3, ¶ 1 (noting that the precise boundaries of the territorial sea depend on how the coastline is defined, the determination of which is specified in detail in the Convention).

The next legal zone is the EEZ, which may not extend further than 200 nautical miles from the coastal State.[80] In this zone, "all States enjoy the freedom of laying submarine cables . . . and other internationally lawful use of the seas related to this freedom, such as the operation of submarine cables," writes Kingsley Ekwere, Senior Lecturer at the University of Port Harcourt, Nigeria.[81]

The next legal zone is the continental shelf, which typically is up to a distance of 200 nautical miles from the relevant coastal State.[82] In this zone, all States may lay submarine cables.[83] Furthermore, no coastal State may interfere with the laying and maintenance of such cables in this zone.[84] To reinforce the importance of allowing all States to lay and repair cables in this zone, UNCLOS mandates that States have "due regard to cables . . . already in position."[85] Additionally, the "possibilities of repairing existing cables . . . shall not be prejudiced."[86]

On the high seas, the next zone, consideration of coastal State jurisdiction comes to an end because "[t]he high seas are open to all States," per Article 87 of the UNCLOS.[87] In this zone, coastal and land-locked States have the freedom to lay submarine cables.[88]

a. UNCLOS Fails to Mitigate Threats to the United States' Cables Because of Omissions in the Text of the Treaty and the Fact that United States is not a Formal Party to the Treaty

Even if the United States were a party to UNCLOS, the treaty would fall short of addressing the intentional and unintentional commercial activities most likely to cause significant disruption to the Internet. Firstly, UNCLOS sets too high of a threshold for what sort of activity can be punished. UNCLOS also does not empower States to take proactive action; the treaty's ambiguities and omissions leave some States wondering if their policy responses are permissible under international law.[89] Secondly, it is important to stress that because the majority of breaks take place within waters shallower than 200 meters, an

[80] *Id*. at art. 57.
[81] *See* Ekwere, *supra* note 23, at 165 (2016) (referring to art. 58, ¶ 1 of UNCLOS).
[82] UNCLOS, *supra* note 76, at art. 76, ¶ 1.
[83] *Id.* at art. 79, ¶ 1.
[84] *Id.* at art. 79, ¶ 2.
[85] *Id.* at art. 79, ¶ 5.
[86] *See id*.
[87] *See id.* at art. 87(1).
[88] *See id.* at art. 87(1)(c).
[89] *See id.* at art. 112–15.

international regime focused on deeper waters will have only limited efficacy with respect to protecting the undersea cable system.[90]

UNCLOS specifically addresses injuries, intentional or not, to submarine cables in Articles 113, 114, and 115.[91] The former, as interpreted by the CCDCOE, "implies that the breaking or injury of a cable need only be punished under domestic law if it is 'liable to interrupt or obstruct . . . communications.'"[92] This condition on interruption or obstruction means that attempted cable-breaking may not be punishable under Article 113. The Article has also been interpreted as allowing espionage based on the requirement for disruption to communication;[93] this interpretation could facilitate more intentional cable attacks. The Article also fails to specify that warships have the right to board vessels in international waters suspected of attempting to intentionally damage undersea cables; the result is that naval powers struggle to deter vessels from conducting attacks on cables.[94]

Article 114 specifies that States shall adopt laws to ensure that persons who "cause a break in or injury to another cable . . . bear the cost of the repairs."[95] Article 115 provides that States shall create laws to ensure that owners of ships who sacrifice an anchor, net, or other form of fishing to save a submarine cable are indemnified by the owner of the cable, so long as "the owner of the ship has taken all reasonable precautionary measures beforehand."[96] Note, however, that the indemnity does not include lost profits or catch.[97] This omission discourages fishermen from sacrificing their equipment, especially if they think that the cable break will not be attributed to them; they would rather increase the odds of keeping their catch, then face the certain losses associated with giving up equipment and more. This omission fails to adequately deter unintentional, commercial breaks. Furthermore, Articles 114 and 115 are contingent on States passing domestic legislation regarding the activities in question;[98] this presents another barrier to their enforcement.

---

[90] Wood & Carter, *supra* note 66, at 448.
[91] UNCLOS, *supra* note 76, at art. 113–15.
[92] *See* CCDCOE, *supra* note 5, at 3 (quoting Article 113, UNCLOS).
[93] *See id*. at 4 (tapping an undersea cable would not stop Internet traffic, but merely allow an unintended third party to review that traffic as well).
[94] SUNAK, *supra* note 10, at 17.
[95] UNCLOS, *supra* note 76, at art. 114.
[96] *Id*. at art. 114–15.
[97] *See* DOUGLAS R. BURNETT & LIONEL CARTER, INTERNATIONAL SUBMARINE CABLES AND BIODIVERSITY OF AREAS BEYOND NATIONAL JURISDICTION 22 (2017) (referring to cable protection zones as "generally comply[ing] with UNCLOS.").
[98] *See* UNCLOS, *supra* note 76, at art. 114–15.

The failure of UNCLOS to explicitly cover the extent to which its provisions pertain to non-state actors represents another gap in the treaty. Though UNCLOS refers to "States," a few scholars have read the term to encapsulate the private actors, such as those who control the vast majority of undersea cables.[99] Still, some scholars have interpreted UNCLOS as requiring national legislation for private actors to exercise the freedom to lay undersea cables.[100] Though international treaties generally do not apply to private parties, the exclusion of such parties is unacceptable in the context of an undersea cable system that is almost exclusively privately-owned.[101]

Other gaps in UNCLOS necessitate action by States to protect undersea cables. Robert Beckman, Director of the Center for International Law at the National University of Singapore, stated the protections afforded by UNCLOS to submarine cables in the high seas, in EEZs, and on continental shelves are "clearly inadequate."[102] The CCDCOE identified two such inadequacies. First, it is unclear if UNCLOS extends legal authority to States to create cable protection zones intended to safeguard the integrity of the undersea cable system.[103] This is problematic given that these zones are designed to prevent the unintentional, commercial breaks in relatively shallow water that account for such a high percentage of [104] Second, it is it is unclear if attempted damage to an undersea cable falls within the provisions of UNCLOS.[105] Note, however, that some stakeholders regard the prohibition against the infliction of damage to cables as a matter of customary law.[106] Third, UNCLOS fails to cover "the intentional theft of submarine cables in maritime zones outside of sovereignty."[107] That's why

---

[99] 3 MYRON NORDQUIST ET AL., UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY, 264 (Martinus Nijhoff et al. eds., 1995).
[100] *See* RAINER LAGONI, LEGAL ASPECTS OF SUBMARINE HIGH VOLTAGE DIRECT CURRENT (HVDC) CABLES 12–13 (1998).
[101] *See* ICPC, *supra* note 14.
[102] ROBERT BECKMAN, SUBMARINE CABLES–A CRITICALLY IMPORTANT BUT NEGLECTED AREA OF THE LAW OF THE SEA 13 (2010), https://cil.nus.edu.sg/wp-content/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables-rev-8-Jan-10.pdf.
[103] *See* CCDCOE, *supra* note 5, at 5; *see also* BECKMAN, *supra* note 102, (citing Article 21(1)(c) of UNCLOS and noting that "UNCLOS gives coastal States the power to impose restrictions on the right of innocent passage in order to protect submarine cables."); BURNETT & CARTER, *supra* note 97, at 21 (referring to cable protection zones as "generally comply[ing] with UNCLOS.").
[104] ICPC, *supra* note 14; *infra* Section V.
[105] *See* CCDCOE, *supra* note 5, at 3.
[106] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 252–53 (Michael N. Schmitt ed., 2017) [hereinafter "TALLINN MANUAL 2.0"].
[107] *See* BECKMAN, *supra* note 102, at 15.

Beckman calls on States to take it upon themselves to fill in the blanks left by UNCLOS;[108] some of his suggestions will be discussed in Sections V and VII.

The textual and scholarly analysis of UNCLOS reveals that it does not adequately address the two key threats identified in Section III. If UNCLOS definitively permitted cable protection zones, especially beyond sovereign seas, then States would have greater authority to reduce problematic commercial activity in more territory. The monitoring associated with enforcing cable protection zones, covered in more detail below, would likely also deter actors aiming to intentionally damage cables. These attackers would similarly be deterred by UNCLOS penalizing attempted damage of cables and by UNCLOS applying universal jurisdiction over breaking or attempting to break cables. However, universal jurisdiction to enforce those proposed provisions is unlikely because of the arduous process required to amend UNCLOS; any amendment to UNCLOS has to be ratified or acceded to by at least 60 State parties.[109] Even when that threshold is met, the amendment only enters into force for those who accept the amendment.[110] Shortfalls notwithstanding, UNCLOS marks an improvement on the prior reliance on customary law to protect the undersea cable system.

UNCLOS, amended or not, can only have a marginal effect on protecting the undersea cable system from the perspective of the United States. The nation has not ratified UNCLOS.[111] Consequently, scholars such as James Kraska of the U.S. Naval War College argue that the United States is missing out on an opportunity to have a more stable legal framework when acting in the continental shelf and beyond.[112] After all, UNCLOS and related conventions were developed in direct response to the uncertainties associated with customary law—"practices considered legally required by most nations," as defined by David B. Sandalow in a policy brief for the Brookings Institution[113]—to govern the oceans. Despite the United States Senate opting not to sign UNCLOS, President Reagan issued an Ocean Policy Statement indicating the nation's intent to generally follow the Convention.[114] Sandalow notes that President Reagan's intentions, as good as they

---

[108] *See id*. at 13.
[109] *See* UNCLOS, *supra* note 76, at art. 313(1).
[110] *See id*.
[111] *See* William Gallo, *Why Hasn't the US Signed the Law of the Sea Treaty?*, VOICE OF AM. (June 6, 2016, 7:00 PM), https://www.voanews.com/a/united-states-sign-law-sea-treaty/3364342.html [https://perma.cc/72NN-A8JT].
[112] *See id.*
[113] *Id.*
[114] *Id*.

may have been, still do not afford the United States all of the benefits made available to nations that have formally ratified UNCLOS.[115]

b. Other Sources of International Law and Norms Offer Only Limited Protection to the United States' Cable System Due to Being Outdated or Non-binding

Because the United States is not a party to UNCLOS, it may cite prior international agreements when seeking to protect the undersea cable system.[116] For instance, the United States may still invoke the Convention for the Protection of Submarine Telegraph Cables (1884 Convention).[117] The United States, as interpreted by the Working Group, regards the provisions of the 1884 Convention as customary law guaranteeing to all states "unique freedoms to lay, maintain, and repair submarine cables."[118] The 1884 Convention, though, provides comparatively fewer protections than UNCLOS; "[t]he [1884 C]onvention," as stated by the CCDCOE, "only focuses on undersea cables located in the high seas."[119] The 1884 Convention does make it a punishable crime "to break or injure a submarine cable, willfully or by culpable negligence, in such a manner as might interrupt or obstruct telegraphic communication."[120] However, the effect of this provision is limited because the 1884 Convention does not apply to situations of armed conflict; thus making it less responsive to threats posed by actors seeking to intentionally damage cables.[121]

This review of international law, as it pertains to the United States, reveals that the nation can only marginally rely on those conventions to combat threats to the undersea cable system. Ultimately the United States has a limited range of legal options from international law to reduce the occurrence of unintentional, commercial threats to the system and to stem the likelihood of actors intentionally attacking the system.

The Tallinn Manual 2.0 represents another international agreement that shapes norms pertaining to the undersea cable system. Developed by the Cooperative Cyber Defense Center of Excellence (CCDCE) within the North

---

[115] *See id*.
[116] CCDCOE, *supra* note 5, at 4 (noting that UNCLOS supersedes many aspects of the Submarine Cables Convention, but pointing out that "[s]tates not party to UNCLOS could, however, continue to invoke the Submarine Cable Convention").
[117] *See id*.
[118] WORKING GROUP REPORT, *supra* note 9, at 8.
[119] CCDCOE, *supra* note 5, at 4.
[120] 1884 Convention, *supra* note 75, at art. 2.
[121] *Id.* at art. 15.

Atlantic Treaty Organization (NATO), the Manual sets forth that customary international law prohibits the infliction of damage to an undersea cable; however, this prohibition would not apply in an armed conflict.[122] According to Garrett Hinck, the writers of the Tallinn Manual 2.0 have specified that States have the right to create cable protection zones within their territorial seas, but beyond that "there is no equivalent clear norm with respect to either the EEZ or continental shelf, and certainly not for the high seas."[123]

Notwithstanding the guidance the Tallinn Manual 2.0 provides, it has limited legal value. The Manual is not binding, but rather it "must be understood only as an expression of the opinions of the two International Groups of experts as to the state of the law," as expressed in the document's introduction.[124] Members of NATO are not bound by the Manual; the Manual does not even reflect NATO's official policies.[125] Instead, the Manual is thought of as a restatement of international laws related to cyberspace, informed by a broad range of international law scholars.[126]

In sum, the Manual does not formally bolster the means by which the United States can reduce unintentional, commercial activity and combat actors intentionally targeting cables.

c. Private Actors Have Proactively Tried to Respond to the Threats to the Undersea Cable System but Lack the Authority and Capacity to Fully Mitigate the Threats

Industry norms help fill some of the holes left by international agreements—especially in the context of unintentional, commercial activity. The ICPC, for instance, has offered several recommendations to reduce the vulnerability of the system. Sample recommendations include specifying the proper distance between cables, outlining the criteria for crossing cables and pipelines, and standards for repairing and installing cables.[127] Several countries have opted to make ICPC standards a formal part of their undersea cable governance. China and the United Kingdom, by way of example, have followed

---

[122] TALLINN MANUAL 2.0, *supra* note 106, at 252–53, 256.
[123] Hinck, *supra* note 7 (citing TALLINN MANUAL 2.0, *supra* note 107, at 256).
[124] TALLINN MANUAL 2.0, *supra* note 106, at 2–3.
[125] *See id*.
[126] Eric T. Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 738, 740 (2017) (citing TALLINN MANUAL 2.0).
[127] WORKING GROUP REPORT, *supra* note 9, at 8–9 (citing ICPC Recommendations 2 No. 10, 3 No. 10, 4 No. 8, 6 No. 8A).

ICPC standards and identified specific minimum separation distances to protect submarine cables.[128]

The North American Submarine Cable Association (NASCA) has also taken steps to support the undersea cable system. NASCA runs cable awareness programs that share the route position list data with commercial fishermen and government agencies; this list has the location information of undersea cables as a way to reduce anchoring- and fishing-related risks to the undersea cable system.[129] Representatives of NASCA further contribute to the security of the undersea cable system through presentations on policy ideas related to increased protection.[130]

Regional committees (such as NASCA) have stepped in to fill regulatory and legal gaps. These committees formed in the late 1990s and early 2000s in response to a "boom" in the undersea cable industry, as labeled by Robert Wargo, who served as President of NASCA.[131] Committees generally formed on a regional and as-needed basis; for instance, the Oceania Submarine Cable Association formed in 2010 and disbanded in 2011.[132] Committee memberships have typically included power and telecommunications cable owners, operators and suppliers; some also featured regulators and government officials.[133] As a result of insufficient government regulations, the committees formed, in part, "to ensure that no cable owner agreed to permit conditions that were technically infeasible and would then need to be agreed to by all others seeking approval at the same time."[134] Wargo noted that the committees also filled a gap left by ICPC in resolving local or domestic problems.[135] The United States is not a formal member of NASCA nor of any specific regional committee;[136] therefore, these outlets do not currently present an opportunity for a centralized response to the main threats to the undersea cable system in the United States.

Not all industry collaboration has necessarily advanced the integrity of the undersea cable system. Case in point, NASCA did not support efforts by the

---

[128] *Id.* at 10.
[129] *Id*. at 9.
[130] Robert Wargo, *The Role of Regional Cable Protection Committees in the Protection of Submarine Cables*, YUMPU, https://www.yumpu.com/en/document/read/18880804/undersea-cables-in-the-south-china-sea-centre-for-international (last visited Oct. 17, 2021).
[131] *Id.* at 1, 4.
[132] *Id.* at 2, 4, 6.
[133] *Id.* at 2.
[134] *Id.* at 4.
[135] *Id*.
[136] *Id.* at 2–3, 5.

Canadian government to group underseas cables and pipelines, even identifying the efforts as inconsistent with Canadian law and historical practices.[137] NASCA representatives have also exploited jurisdictional differences in regulations among states in the United States to pass "cable friendly" provisions.[138]

V. The United States Should Learn from the Undersea Cable Laws of Other Nations to Better Protect its own Portion of the System

Because of the inadequacies of UNCLOS, in particular, and the international legal and regulatory environment, in general, there is a need for affirmative action by the United States to protect the undersea cable system. Notably, the United States is not alone; according to Beekman "the laws and regulations of most states on the protection of submarine cables are inadequate."[139] A few states, however, have taken meaningful action against the two main threats. Laws and regulations adopted by Australia, New Zealand, and Sweden offer templates for the United States to consider.[140]

Due to the substantial number of cables along the US and the nation's complicated federal system, there is no peer country to study with respect to undersea cable policy. For instance, the policy lessons learned from New Zealand are of limited value because the country has fewer cables than the United States;[141] similarly, China's approach to undersea cable protection is of limited value to the United States because of the centralized structure of China's government and its more uniform approach to coastal and ocean law.[142] Consequently, the United States will have to glean only the most applicable lessons from other countries addressing the threats to the undersea cable system.

Australia and New Zealand created cable protection zones that prohibit certain activities from occurring around undersea cables. Australia created the first such zones in 2007.[143] In consultation with industry stakeholders, Australian authorities created zones near Sydney which prohibit activities of the highest risk

---

[137] *Id.* at 5.
[138] *Id.*
[139] BECKMAN, *supra* note 102, at 13.
[140] WORKING GROUP REPORT, *supra* note 9, at 10.
[141] *Id.* at 56.
[142] *See, e.g.,* Eli Huang, *China's cable strategy: exploring undersea cable dominance*, AUSTL. STRATEGIC POL'Y INST. (Dec. 4, 2017), https://www.aspistrategist.org.au/chinas-cable-strategy-exploring-global-undersea-dominance/ [https://perma.cc/RT3H-ZZ5Y].
[143] Australian Communications and Media Authority, *Protection Zones Declared for Submarine Telecommunications Cables off NSW Coast*, ACMASPHERE, Aug. 2007, at 8–9 [hereinafter ACMA]; s*ee also* Submarine Cables and Pipelines Protection Act 1996 (N.Z.).

to cables such as "sea-bottom trawl fishing, anchoring, sand-dredging and dumping."[144] Zones may only be created around cables that are of national significance.[145] In the case of the first zones, each contained "nationally significant high-capacity cables linking Australia to global communications systems," as described by the Australian Communications and Media Authority (ACMA).[146] Another zone off the coast of Perth has since been identified.[147]

Cable protection zones, however, do not guarantee that human activity will never disrupt or break a cable. Some limits to the efficacy of cable protection zones are inherent to the policy. The creation of cable zones increases awareness of cable location and, accordingly, allows attackers to more easily target the systems. Cable zones also increase the odds of unintentional breaks caused by placing more cables in a narrower geographic area.[148]

Cable corridors, which create protection zones for cables to be laid, rather than zones around pre-existing cables, suffer from a similar problem as that of protection zones. Another factor mitigating the effectiveness of cable protection zones and corridors is implementation. A lack of proactive monitoring and deterrence by legal authorities around the zones or corridors may render the intended protection moot. This lack of deterrence may have been worsened by the comments of the Australian Federal Police (AFP), explicitly stating that they did not have a responsibility to monitor, nor supervise, the safekeeping of the cable protection zones, and that they lacked the resources to do so.[149]

New Zealand has modeled and improved upon the Australian approach to cable protection zones. In contrast to Australia's three zones, New Zealand has created ten.[150] Unlike Australia, New Zealand has taken a proactive approach to

---

[144] ACMA, *supra* at 8–9; *see also Telecommunications Act 1997* (Cth) (Austl.).
[145] ACMA, *supra* note 144, at 8; *Telecommunications Act 1997* (Cth) (Austl.).
[146] ACMA, *supra* note 144, at 8.
[147] *See* APEC COMM. ON TRADE AND INVESTMENT, REPORT OF THE TRADE POLICY DIALOGUE ON THE TRADE BENEFITS FROM SUBMARINE CABLE PROTECTION 10 (2012), https://www.apec.org/-/media/APEC/Publications/2012/4/Report-of-the-Trade-Policy-Dialogue-on-the-Trade-Benefits-from-Submarine-Cable-Protection/2012_CTI_Trade-Policy_Dialogue_Submarine_Cables.pdf.
[148] *See, e.g.*, Jessica Woodall, *Australia's Vulnerable Submarine Cables*, AUSTL. STRATEGIC POL'Y INST. (May 31, 2013), https://www.aspistrategist.org.au/australias-vulnerable-submarinecables/.
[149] *See* AUSTRALIA COMM. AND MEDIA AUTHORITY, REPORT ON THE OPERATION OF THE SUBMARINE CABLE PROTECTION REGIME 15 (2010), https://apo.org.au/sites/default/files/resource-files/2010-09/apo-nid23392.pdf.
[150] *See Safety Update,* MARITIME N. Z. (Aug. 1996), https://www.maritimenz.govt.nz/commercial/safety/safety-updates/navigation-stability/cables-pipelines.asp (listing locations of ten New Zealand cable protection zones).

enforcing prohibitions related to the zones.[151] A report by the Australian Strategic Policy Institute commended the impressive enforcement regime employed by their neighbors: "Protection officers and Maritime Police [in New Zealand] not only patrol their zones with ships and helicopters, in some cases they operate for up to 24 hours a day."[152]

FIGURE 5: Map of a cable protection zone in New Zealand.[153]

Though these two nations have experienced success with their zones, zones and corridors are "not generally implemented [by countries around the world]," despite the fact that "they could reduce unintended cable damage."[154] Where zones have been instituted and effectively enforced, instances of cable breaks have decreased to near zero.[155] Given the success of these zones, it makes sense that the two oceanic nations are not alone in having adopted cable protection zones; other countries with zones include Denmark, Uruguay, and Colombia.[156]

---

[151] *See*, *e.g.*, Submarine Cables and Pipelines Protection Act 1996, pt. 3 (N.Z.) (approving of government purchases of additional maritime surveillance equipment to assist with enforcement of the act).
[152] Woodall, *supra* note 148.
[153] CARTER ET AL., *supra* note 22, at 37 (exhibiting cable protection zone map from Telecom New Zealand in Figure 5.7).
[154] CCDCOE, *supra* note 5, at 3.
[155] BURNETT & CARTER, *supra* note 97, at 21.
[156] *Id*. at 14.

Another approach to reduce the likelihood of cable damage is to increase the penalties for any such violation. Australia and New Zealand have modeled this approach by imposing stiff penalties for violating their cable protection zones, and for causing damage to an undersea cable. In Australia, for example, a person who "engages in conduct . . . that results in damage to a submarine cable [that is in a cable protection zone]" may be imprisoned for ten years.[157] Sweden has also imposed a legal structure likely to deter damage where owners of a cable that cause damages to another cable must cover the repair costs.[158] New Zealand has also imposed penalties with similar potential to deter damage.[159] And as Article 113 of UNCLOS provides criminal sanctions for those who willfully or with culpable negligence injure undersea cables, China has also adopted cable protection legislation. In contrast, however, this legislation has done little, if anything, to deter injurious behavior.[160] Both China's struggles with reducing breaks and the inadequacies of Australia's enforcement regime related to its cable protection zones suggest that effective enforcement is a necessary condition to protecting the undersea cable system.

Other less punitive policies to reduce the likelihood of damage to undersea cables include information-sharing regimes. For instance, Australia and New Zealand have tasked their governments with providing cable route information and coordinating with the fishing and maritime industries.[161] National security strategists, such as the Director of National Strategic Studies in the United States, have acknowledged the importance of information sharing.[162] In other maritime contexts, national security entities have set up an "unclassified, multinational, freely shared" automatic identification system to track merchant ships. A similar system for undersea cables would help reduce cable disruptions.[163]

---

[157] *Telecommunications Act 1997* (Cth) (Austl.).
[158] ACT ON THE OBLIGATION TO PAY COMPENSATION FOR DAMAGE TO SUBMARINE CABLES AND PIPELINES (Svensk författningssamling [SFS] 1996:518) (Swed.).
[159] WORKING GROUP REPORT, *supra* note 9, at 10.
[160] *See* BURNETT & CARTER, *supra* note 97, at 21, n.82 (reporting that "China in the years 2008–2015 [had] an average number of about 26 cable faults per year, the highest of any state").
[161] *Telecommunications Act 1997* (Cth) sch 3A pt 2 div 2 sub-div A para 8 (Austl.) (stating that the "Location of submarine cable to be specified in declaration"); Submarine Cables and Pipelines Protection Act 1996, pt 2 s 12 (N.Z.) (allowing cable protections to apply "differently in respect of specified methods of fishing").
[162] MICHAEL MATIS, THE PROTECTION OF UNDERSEA CABLES: A GLOBAL SECURITY THREAT 3 (U.S. Army War College 2012) (describing the importance of information-sharing in underwater cable protection and acknowledging Stephen Krotow, Director of National Strategic Studies Department, as project advisor).
[163] *Id.* at 26.

On the whole, laws, regulations, and norms surrounding protection of undersea cables reflect difficult trade-offs between commercial fishing, navigation, and undersea cables. Scholars David R. Burnett and Lionel Carter recommend that any tinkering with this balance be taken on with "[g]reat care, careful thought, and evidence justifying the need and the risk of intended consequences [associated with any change]."[164] This recommendation, though, likely does not apply to nations in desperate need of modern legislation and regulation, including the United States, which Burnett and Carter criticize for its antiquated "telegraph era statutes based on the 1884 Cable Convention that are historical relics with little practical utility."[165]

VI. The United States Legal Framework and its Policy Responses to System Threats are Insufficient

With limited options through international law, and having failed to implement best practices gleaned from policies implemented elsewhere, there is a tremendous amount of room for improvement in the United States' legal and regulatory framework pertaining to undersea cables. The time to realize these improvements is now. Increasing development in the United States coastal and marine areas threatens the integrity of the undersea cable system.[166] These activities, if left unregulated, threaten the installation of cables, threaten to limit the speed of effective and efficient cable repairs, and threaten to detrimentally alter the course of cables by effectively requiring that they cluster together, thereby "magnifying[ing] the risks of damage and communications outages across multiple systems due to particular natural or man-made events."[167]

a. The Manifold Federal Agencies with Partial Authority Over Undersea Cables Hinder the Development of a Comprehensive Protection Regime

United States laws and regulations fall short in four main ways. U.S. laws and regulations have fallen short by way of, first, a lack of clarity regarding which agency or agencies should lead on undersea cable protections; second, insufficient penalties to deter behavior likely to result in broken undersea cables; third, insufficient coordination among federal, state, and local governments regarding specifying and enforcing standards and regulations; and, fourth, as briefly

[164] BURNETT & CARTER, *supra* note 97, at 23.
[165] *Id.* at 21.
[166] WORKING GROUP REPORT, *supra* note 9, at 5.
[167] *Id.*

discussed above, private actors, such as Big Tech companies, bearing too much responsibility for protecting the undersea cable system.

Though the United States Federal Government has recognized the importance of undersea cables, no agency has taken ownership over the protection of the system. Importantly, the government has labeled undersea cables as critical infrastructure.[168] This designation suggests that the government would formalize its institutional response to protecting the system, yet the Working Group determined that "no U.S. federal agency has transposed th[e] finding [of undersea cables as critical infrastructure] in practical terms to adopt or enforce cable-protection standards or policies."[169] Instead, as noted by the Office of the General Counsel within the National Oceanic and Atmospheric Administration (NOAA), "a number of U.S. agencies have authority to regulate the laying and maintenance of cable off of [the] nation's shores."[170] This observation is important in two respects: first, it acknowledges that many agencies have a role in undersea cable regulations and laws; and, second, it specifies the existence of authority of several agencies over the undersea cable system, but not an obligation on any one agency to lead on policy formulation and implementation.

An exhaustive review of the role of each United States federal agency with ties to the undersea cable system is beyond the scope of this paper. Still, even a partial overview reveals the fragmented approach taken by the United States government. NOAA has the authority "to regulate whether and how proposed submarine cables may be installed in National Marine Sanctuaries."[171] NOAA, as discussed below, also plays a role in administering the Coastal Zone Management Act ("CZMA").[172]

The United States Army Corps of Engineers also has authority over undersea cable laying—at least on the seabed of the outer continental shelf—via section 10 of the Rivers and Harbors Appropriations Act of 1899.[173] This authority often entails weighing the national security implications of laying a specific cable.[174] Another agency, the Federal Energy Regulatory Commission, also has authority over some undersea cables proposed to rest on the continental

---

[168] *Id.* at 11.
[169] *Id.*
[170] NOAA Office of General Counsel, *Submarine Cables—Domestic Regulation*, NOAA (July 8, 2019), https://www.gc.noaa.gov/gcil_submarine_cables_domestic.html.
[171] *Id.* (citing 16 U.S.C. § 1435(a) (2000)).
[172] *See infra* Section VI(c).
[173] NOAA, *supra* note 170 (referring to 33 U.S.C. § 403, as amended by the Outer Continental Shelf Lands Act of 1953 (OCSLA), 43 U.S.C. § 1333(e)).
[174] 33 C.F.R. § 320.2; 33 C.F.R. § 320.4(j)(2).

shelf.[175] The Department of the Interior may also play a role in shaping the nature of a proposed cable; at times, its specific grant of authority may overlap with that of the Army Corps of Engineers.[176]

The Federal Communications Commission ("FCC") plays a pivotal role in undersea cable policy and regulation. It has the authority to issue licenses for "any submarine cable directly or indirectly connecting the United States with any foreign country, or connecting one portion of the United States with any other portion thereof."[177] Approval of an undersea sea cable license application is contingent upon the applicant providing information related to ownership of the cable, certain reporting requirements, and conditions imposed on each cable landing license.[178]

Occasionally, agencies or their sub-units act in informal capacities to assist initiatives meant to protect the undersea cable system. For example, the Bureau of Ocean Energy Management ("BOEM") has partnered with the U.S. Coast Guard to enforce an informal agreement barring installing wind energy structures within one nautical mile of a traffic separation scheme.[179] Additionally, at times, the U.S. Coast Guard will create safety zones around energy exploration and exploitation facilities on the OCS of the United States.[180]

This brief overview of the agencies with some stake in the undersea cable system reveals a series of overlapping authority. Absent more clarity around which agency is responsible for protecting the undersea cable system, it is likely that the current approach will fail to protect the system in the event of significant disruptions—regardless of the intentionality of the responsible party. At the federal level alone, overlapping jurisdictions make it harder to implement cable protection zones and other related legal responses to the threats posed by unintentional, commercial activity and intentional attacks.

b. Insufficient Penalties for Breaking Cables Fail to Deter Unintentional Breaks

Underneath the morass of potential agency regulations rests the federal law prohibiting certain activities related to undersea cables. The main law on the

[175] 16 U.S.C. § 792–823(a).
[176] 33 U.S.C. § 403; 43 U.S.C. § 1333(e).
[177] 47 U.S.C. § 34.
[178] 47 C.F.R. § 1.767.
[179] WORKING GROUP REPORT, *supra* note 9, at 10.
[180] *Id*.

books serves as an inadequate deterrent to problematic behavior from commercial actors and state and non-state attackers. According to the Submarine Cable Act, enacted in 1888, "[a]ny person who shall willfully and wrongfully break or injure, or attempt to break or injure . . . a submarine cable in such a manner as to interrupt or embarrass, in whole or in part, telegraphic communication" shall be liable for as many as two years in prison and/or a fine of up to $5,000.[181] As reported by the Working Group Report, the penalties associated with causing damage to a submarine cable are "unlikely to deter negligent or willful damage and do not even cover the cost of the repair."[182] The United States has not updated its penalty amount for cable damage for more than 125 years.[183] It is unlikely that attackers even weigh prison time and fees when planning their acts; this is even more likely to be the case when law enforcement has few means and a diminished incentive to effectuate enforcement.[184]

There are other laws related to damage caused by commercial actors to undersea cables lack sufficient deterrent power. Federal law holds fishing vessels accountable by subjecting fishermen who fail to keep their equipment from interfering with or damaging submarine cables to punishment;[185] the law specifies a fine of up to $250 and a prison term for as many as ten days for fishing-related damage. The law also obligates fishing vessels to remain a minimum distance from vessels engaged in laying cables or buoys indicating the position of a cable.[186]

c. Federalism Undermines a Comprehensive Approach to Undersea Cable Protection Because States Often have Policy Priorities that Conflict with Protecting the System

Coastal states influence undersea cable protections and regulations. As a consequence of the Submerged Lands Act, each coastal state has authority over the three nautical miles of seabed off their coast.[187] Nevertheless, many states have yet to take substantial action to protect undersea cable systems. As detailed by the Working Group Report, "no U.S. federal, state, or local government agency has promulgated laws or regulations establishing default or minimum separation distances," referring to the minimum separation distance between an

[181] 47 U.S.C. § 21.
[182] WORKING GROUP REPORT, *supra* note 9, at 8.
[183] *See id*. at 10.
[184] Scott Coffen-Smout & Glen J. Herbert, *Submarine Cables: A Challenge for Ocean Management*, 24 MARINE POL'Y 441, 444 (2000).
[185] *See* WORKING GROUP REPORT, *supra* note 9, at 8.
[186] *Id*.
[187] 43 U.S.C. §1301.

existing undersea cable and any other marine activity in the absence of "any mutual agreement to allow the activity in closer proximity to the submarine cable."[188] These mandated distances could reduce the frequency of commercial activities leading to cable breaks; for instance, submarine cables that are a part of the Internet would have sufficient berth from cables that may be relaying power from offshore wind farms.

Administered by NOAA, the CZMA also creates a role for states to play in undersea cable policy.[189] Under the CZMA, the nation's coastal resources ought to be balanced between economic development and coastal conversation.[190] Determining that balance must be done in coordination with the states: "no federal agency may grant a license to conduct an activity affecting a coastal area until a state concurs or is presumed to concur with the applicant's certification that a proposed activity is consistent with the state's coastal management plan."[191] This means that individual states could disrupt efforts by the Federal Government that either stem commercial activity or foster it. States could act as individual protectors of cables by creating coastal management plans that require certain protections for cables.

The ability of states to shape undersea cable policy is not lost on industry actors. States have become targets of industry groups for regulatory capture. Former NASCA President Wargo made that clear in a presentation that highlighted NASCA working with various states to "get more 'cable friendly' regulation."[192] As a counterpoint, some states have been more proactive than others in developing and enforcing spatial planning schemes.[193] Still, a state-by-state effort to address the threats posed by commercial actors to the undersea cable system likely falls short of the sort of comprehensive policy solution necessitated by infrastructure of this importance.

Notwithstanding the power held by states to affect policies related to commercial actors, they lack the sort of coordination to respond to the threats posed by attackers. Federal actors are better suited to determine the nation's plan to reduce breaks caused by attackers—a plan that necessarily raises the sort of foreign policy questions usually left to the Federal government. At this point,

---

[188] WORKING GROUP REPORT, *supra* note 9, at 9.
[189] NOAA, *supra* note 170, at 2.
[190] *Id.*
[191] *Id*. (referencing 16 U.S.C. § 1456(c)(3)(A)).
[192] *See* Wargo, *supra* note 130, at 8.
[193] *See* WORKING GROUP REPORT, *supra* note 9, at 11 (pointing to the Mid-Atlantic Council on the Ocean and the Northeast Regional Ocean Council).

though, even the Navy has yet to adopt a formal plan for the protection of the undersea cable system.[194]

d. Private-Sector Stakeholders Have Succeeded in Creating Patchwork Protections of the Undersea Cable System, but these Protections are far from Comprehensive

Insignificant legal protections have thus far forced private stakeholders, such as Big Tech companies like Google, to take the protection of the undersea system into their own hands. Submarine cable operators, for example, have had a relatively high degree of success in mitigating damage to cables by burying and armoring cables, instituting cable awareness campaigns, and compensating fishermen for any gear snagged by the cables.[195] Cumulatively, these tactics can reduce threatening commercial activity.

In a similar fashion, regional committees of fishermen and submarine cable owners have often reached agreements around how to divvy up the seabed.[196] Thanks to these agreements, cables in many areas have been placed outside of highly fished areas, thereby decreasing the risk of commercial damage to cables.[197] For example, the Oregon commercial trawl fisherman collaborated with numerous other private companies to create "the Oregon Fisherman's Undersea Cable Committee Agreement," which represented the first effort by two private stakeholder groups to "discuss, describe, and delineate their shared use of a community resource—the ocean."[198] Nevertheless, these "self-help" mechanisms, as described by the Working Group Report, have proven to be "wholly inadequate" for ensuring the protection required for such an important piece of the nation's infrastructure.[199] Moreover, to an even greater extent than states, private actors are limited in their ability to respond to attackers because they generally lack the authority to respond to attacks by foreign and non-state actors.[200]

---

[194] Hinck, *supra* note 7, at 2.
[195] *See* WORKING GROUP REPORT, *supra* note 9, at 5.
[196] *See id*. at 11.
[197] *See id*.
[198] *About OFCC, Or. Fisherman's Cable Comm*., OR.'S FISHER CABLE COMM., http://www.ofcc.com/about_ofcc.htm (last visited Sept. 19, 2021).
[199] *See* WORKING GROUP REPORT, *supra* note 9, at 12.
[200] Momentum may be building to allow private actors to more proactively engage with foreign and non-state actors. For instance, Congress has considered amendments to the Computer Fraud and Abuse Act that would allow private companies to "hack back" foreign and non-state actors that infiltrate private computers. Shannon Vavra, *Congress to take another stab at 'hack back'*

United States federal agencies have helped private actors with some cable protection projects and initiatives, but only on a reactive basis; it follows that the agencies, according to the Working Group, place "the burden on the submarine cable operator[s] to justify a particular method of protection."[201] These ad hoc and private measures should be replaced by a set of laws and regulations that ensure the integrity of the undersea cable system in a comprehensive manner—addressing both attackers and commercial actors.

VII. The New United States Presidential Administration Should Adopt Short- and Long-Run Responses to the Threats to the Undersea Cable System

An initial, speedy review of this paper and topic at large could lead one to believe that the United States could significantly contribute to the integrity of the undersea cable system simply by ratifying UNCLOS and creating cable protection zones. Ratifying UNCLOS would improve the regulatory and legal framework of the United States related to the system by affording the nation standing in conversations about amending the Convention as well as providing the nation with more legal authority to take actions related to the breaking of undersea cables. Creating cable protection zones, in theory, would indicate that the United States was adopting a best practice that has shown great results in reducing undersea cable breaks in nations such as New Zealand, where several zones have been created and where enforcement is high.

a. Neither Ratifying UNCLOS nor Creating Cable Protection Zones Will Adequately Address the Threats to the Undersea Cable System in the United States

In practice, neither ratifying UNCLOS nor attempting to adopt cable protection zones would make much of a difference in the occurrence of cable breaks caused by unintentional, commercial activities, or intentional activities in the United States. Even if the United States ratified UNCLOS and adopted legislation to implement Articles 113, 114, and 115, the efficacy of that legislation hinges on effective monitoring; as is the case with cable protection zones.[202] The United States, in the context of effectively monitoring cable break

legislation, CYBERSCOOP (Jun. 13, 2019), https://www.cyberscoop.com/hack-back-bill-tom-graves-offensive-cybersecurity/ (noting that some cybersecurity experts regard the authorization of private actors to "hack back" as a dangerous idea).

[201] WORKING GROUP REPORT, *supra* note 9, at 10–11.

[202] *See* BURNETT & CARTER, *supra* note 97, at 21.

activities, is much more akin to China than New Zealand. In other words, like China, the United States has too many cables and insufficient resources to effectively monitor cable-breaking activity;[203] on the other hand, New Zealand has three cables, which the nation relies on for all of its international data traffic.[204, 205]

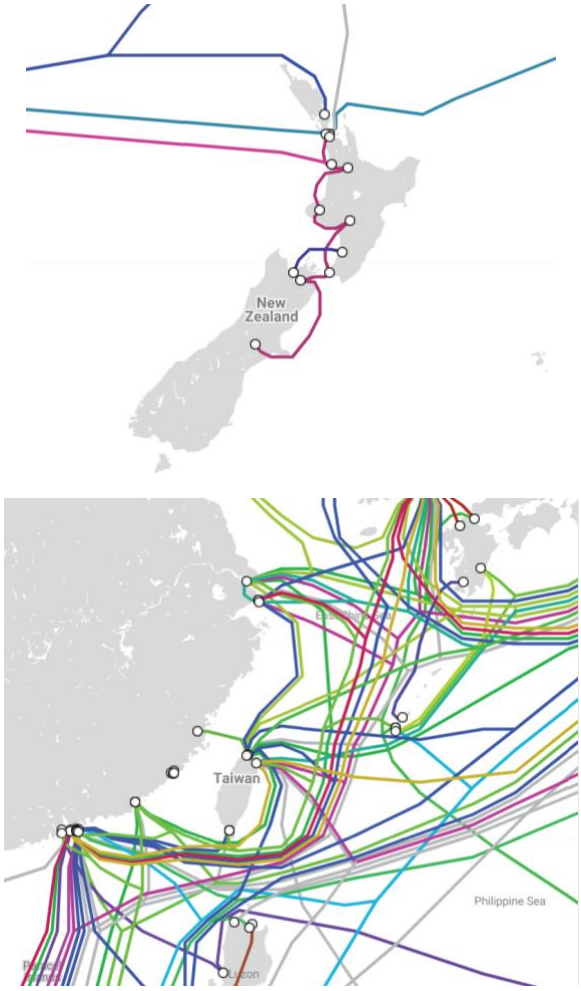


FIGURE 6: Undersea cables off of New Zealand (upper) and China (lower) as of January 24, 2021.[206]

[203] *See* WORKING GROUP REPORT, *supra* note 9, at 1.
[204] TELEGEOGRAPHY, *supra* note 1.
[205] SUNAK, *supra* note 10, at 18.
[206] TELEGEOGRAPHY, *supra* note 1.

The absence of effective enforcement via effective monitoring will render both UNCLOS-related legislation and cable protection zones insufficient to maintain and improve the integrity of the undersea cable system. What's more, unlike New Zealand, the United States holds a significant position in geopolitics. It follows that the United States must be far more attentive to the downside of openly sharing the location of its cables via cable protection zones; identifying the location of its cables could attract the attention of actors seeking to intentionally break cables. So, whether the cable protection zones were designed for pre-existing or future cables, the issue of actors seeking to cause intentional damage being notified of the location of the cables still proves problematic.

However, some of the shortfalls of cable protection zones could be remedied by scaling back the scope of the zones. For example, the British Parliamentarian Sunak has advocated for smaller zones around the most important cables and for targeting monitoring resources on these locations.[207] The United States may struggle to identify such narrow zones, given that the majority of cables are privately owned and the manifold cables lining the coast of the United States. What criteria would justify affording some cables greater protection than others? Some factors, such as the amount of Internet traffic carried on specific cables, may help identify the most important zones for protection. The process for creating a specific list of factors and outlining specific zones would likely be subject to costly and time-intensive litigation. The vulnerability of the undersea cable system to threats of unintentional, commercial, and intentional breaks requires a faster policy response.

Note also that this paper is not actively opposing the ratification of UNCLOS, but only suggests that doing so would have a limited impact on protecting the undersea cable system. The fact that U.S. states would still retain significant authority over the shallow waters prone to breaks caused by commercial activity reinforces the limited efficacy of UNCLOS.[208]

Finally, the politics of ratifying UNCLOS or adopting cable protection zones could impose a substantial barrier to realizing either goal. Though bipartisan support for ratifying UNCLOS has existed since at least the early 2000s,[209] oppositional political forces as well as political inertia have thwarted ratification. Similar political coalitions could likely mount a successful campaign

---

[207] SUNAK, *supra* note 10, at 18.
[208] *See* CARTER ET AL., *supra* note 22, at 44.
[209] *See, e.g.,* David D. Caron & Harry N. Scheiber, *The United States and the 1982 Law of the Sea Treaty*, AM. SOC'Y INT'L L. (June 11, 2007), https://www.asil.org/insights/volume/11/issue/16/united-states-and-1982-law-sea-treaty.

against cable protection zones as well. One such coalition member could be NASCA, which has already proven capable of pushing back against cable protections that did not meet its standards.[210]

b. Gathering and Sharing Information Related to Undersea Cable Threats Will Immediately Increase Deterrence by Making Attribution of Breaks Easier

Given the importance of the severity and likelihood of getting caught breaking a cable to reducing the frequency of breaks, the United States should review the remaining policy options through a lens that promises the greatest deterrent effect to actors likely to unintentionally or intentionally break cables. With that in mind, the United States should focus on three policy goals: information gathering, information sharing, and increasing penalties.

Regarding information gathering, the U.S. should institute a new requirement to include sensors on all undersea cables and should pursue international agreements and domestic regulations to monitor ship locations. Undersea cables are "located hundreds if not thousands of miles from anywhere or anything that can detect and monitor the presence of a hostile maritime actor," based on Sunak's research.[211] Consequently, Sunak recommends that nations mandate cable laying companies to "place relatively cheap sensors that detect sonar frequencies near key undersea infrastructure and along cable routes. If the sensors were tripped, they could alert nearby coast guard or navy assets."[212]

In the context of the United States, the FCC could realize this information gathering strategy by mandating that cable operators include their use of sensors in any license for an undersea cable. This small step would turn the agency's licensing process into an effective tool for improving the nation's response to the primary dual threats to the system; of course, there would need to be follow up efforts to ensure that license recipients installed the sensors when laying their cables. Private owners of these cables would likely comply with this sensor requirement if they knew that the resulting information would help them recover any costs associated with repairing a break in their cable.

---

[210] *See* Wargo, *supra* note 130, at 9.
[211] SUNAK, *supra* note 10, at 23.
[212] *Id.* at 35 (citing Robert Martinage, *The Vulnerability of the Commons*, FOREIGN AFFAIRS, January/February 2015); *see generally Telecommunications Act 1997* (Cth) (Austl.); Submarine Cables and Pipelines Protection Act 1996 (N.Z.).

In the event that the United States is unable to rally an international coalition to create an information gathering system or pass similar domestic legislation, the private sector may be able to adopt its own standards to achieve the same effect. The ICPC, for instance, could mandate that its members include sensors on their cables as a condition of their membership. Of course, the ICPC may seek federal funds to help cover the costs of such a requirement; asking Congress for money would likely be easier than asking the gridlocked body to pass meaningful legislation. This approach would benefit from being easier and faster to implement. However, an international treaty or domestic law would likely be easier for the state and federal authorities to enforce, which, as discussed in Section V, is imperative to an effective regime. With the protection of the undersea cable at stake, both short- and long-term solutions ought to be pursued.

However, the sensors are implemented, to ensure a high likelihood of identifying the person or entity responsible for a break observed by a cable's sensors, it is essential to locate the ship nearest to the cable at the time of the break. Australia and New Zealand offer a policy response that, if expanded, could supply that information. In those countries, ships within cable protection zones are required to broadcast their locations to the relevant Coast Guard.[213] This obligation ensures that the Coast Guard can effectively track when ships near and cross cables. The United States should expand this requirement to all boats within its territorial seas, EEZ, and continental shelf—doing so would not interfere with the rights or freedoms of any State to sail in such waters.[214]

On the high seas, the United States should reach agreements with other nations to delineate specific monitoring responsibilities; given that the vast majority of breaks occur within territorial seas and EEZs, it is most important that the United States work with other nations to observe their respective waters.[215]

With this sort of international monitoring, it would be possible to cross reference any break triggered by the cable sensors against the location database. The geographic and data-keeping responsibilities of nations in this monitoring arrangement could be specified in future trade agreements or through international bodies such as NATO or the UN.

---

[213] SUNAK, *supra* note 10, at 18.

[214] *See* BURNETT & CARTER, *supra* note 97, at 71 (indicating that of the four average annual repairs that took place in U.S. waters from 2008 to 2015 three were in the EEZ, and one was in the territorial waters).

[215] *See id*. (indicating that the average number of repairs per year, from 2008 to 2015, in the high seas was just 5; comparatively, China averaged 26 within its territorial waters and EEZ).

The exchange of sensitive information between private and public stakeholders will not be realized without an information sharing regime in place. By way of example, Congress passed the Cybersecurity Information Sharing Act to create a legal safe harbor for companies subjected to cyberattacks to exchange information with government stakeholders.[216] A similar piece of legislation could provide companies that share information related to their undersea cables with certain benefits, so as to increase the odds of them installing the sensors discussed above and sharing trigger events with the government in a timely fashion. For example, the legislation could make the provision of repair costs to the private owner of the cable from the party responsible for the break contingent upon the cable company being a part of the information sharing agreement.

This agreement would also provide the government with assurances that the private companies would not divulge government information collected via national security systems, such as information collected through the Integrated Undersea Surveillance System (IUSS). The IUSS is the Navy's "array of fixed and mobile acoustic arrays that provide its primary means for detecting submarines."[217] By placing the location of submarines and ships into a database with sensor-gathered information related to cables, the odds of identifying the culprit for any cable break would drastically increase. This extensive cooperation would make even the most sophisticated attacker think twice before intentionally breaking a cable and would give pause to commercial actors every time they considered dropping anchor. This legislative solution, though, would take time. It follows that congressional hearings on this topic should commence sooner rather than later.

With information gathering and sharing addressing the likelihood of being caught, increasing the fines associated with breaking a cable is the last remaining aspect of the deterrence equation. The United States must update the penalties associated with intentionally damaging, attempting to damage, and negligently damaging undersea cables. Consider that breaching undersea cable laws and regulations in New Zealand or Australia carries fines of more than US $68,410 and US $342,004, respectively.[218] Comparatively, the corresponding fine in the United States is just $5,000.[219] Although this increase will likely only add to the

---

[216] *See* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. F. CORP. GOVERNANCE (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/#1.
[217] Hinck, *supra* note 7.
[218] *See* SUNAK, *supra* note 10, at 18.
[219] 47 U.S.C. § 21.

deterrence of commercial actors, those actors are still the most likely to cause a break. So, the increase is likely to be a meaningful policy intervention.

This base level fine should be increased and tiered based on several factors. For one, large corporate actors guilty of breaking a cable should face a higher fine than commercial fishermen; this differentiation would help mitigate any political pushback from the organizations representing the latter group. Additionally, the fine should increase based on the level of culpability; for instance, a safe harbor could be created for commercial entities that install specific equipment to assist with location monitoring of ships. Finally, those entities that have repeatedly broken cables should face continually greater fines as their number of violations increase. And, as mentioned above, the culpable party should have to directly compensate the cable owner for the repair costs, so long as the cable owner is a part of the information sharing regime.

VIII. Conclusion

Those nations that are part of UNCLOS should form a coalition to amend Article 113 to remedy the provision's current practical effect. More specifically, as currently written, "when a submarine cable beneath high seas or EEZ is broken or damaged by intentional or reckless conduct, in many cases no crime has been committed under any State's laws" because Article 113 requires States to have incorporated the article into their national laws and most states have not done so based on research by Beckman.[220] This same coalition should also establish universal jurisdiction over persons who intentionally destroy or damage submarine cables; doing so would reflect the reliance of so many States on this system, as well as the increased threat of terrorist acts against the cables.[221]

Other ideas worthy of consideration by the international community include laying more "dark cables," creating a new international treaty penalizing international interference with undersea cables, and mandating minimum levels of CLS security in that same international treaty. Sunak recommended each of these strategies, as well as several others, in his report.[222] Dark cables refer to cables that do not appear on publicly available maps. By staying out of public knowledge, the cables are made more secure against intentional sabotage or

[220] *See* BECKMAN, *supra* note 102, at 13–14.
[221] *Id*.; *see also* SUNAK, *supra* note 10, at 17 (stating "There is a strong argument that international damage is a crime that attracts universal jurisdiction and all states should have jurisdiction over the offender, something that Article 113 does not provide for.").
[222] *See* SUNAK, *supra* note 10, at 34–36.

espionage efforts. Sunak envisions using tax incentives to encourage cable owners to create these clandestine cables.[223]

Sunak also calls for the creation of an entirely new international treaty specifically tailored to meeting the needs of the undersea cable system.[224] Though the prospects of getting the international community to agree on much of anything these days seem dim, this narrowly tailored treaty could bring a sufficient number of major stakeholders together to build momentum toward a new treaty. If legislation incorporating Article 113 into domestic law is any indication of a willingness to take proactive steps to protect the undersea cable system, then even China may be supportive of such a treaty. Of course, private stakeholders would likely sign on as well if the treaty helped them more expeditiously repair their cables. This treaty should also include efforts to inventory and coordinate the use of cable repair resources. Given that there are around 59 cable ships in the world and only half stand ready to conduct emergency repairs, it is essential that these resources are used deliberately by the international community.[225] This would be a marked improvement on the current approach to sharing repair resources: private contracts developed around geographic regions.[226] An international agreement could also incentivize the creation of more such ships, especially if treaty signatories could provide extra funds to ships that reach breaks in the most timely fashion.

Though CLS protection was not the focus of this paper, Sunak makes a convincing case for making CLS a focus of international collaboration. Right now, CLS tend to be concentrated in a few areas in coastal states.[227] Oftentimes, these CLS have little to no security, making them easy targets for attackers. An international agreement could help create standards for keeping these sites safe from threats, ranging from climate change to terrorists. Notably, the FCC could also institute such standards through its licensing authority.

No single policy is capable of mitigating all of the threats facing the undersea cable system. Still, some policies seem more likely than others to deter the actions most commonly associated with breaks in undersea cables. These policies ought to be pursued first, though efforts to form a broader, more

---

[223] *See id*. at 35.
[224] *See id*. at 35–36.
[225] *See* BURNETT & CARTER, *supra* note 97, at 45.
[226] *Id*.
[227] *See, e.g.*, SUNAK, *supra* note 10, at 6 ("UK cables are highly concentrated in a small number of landing sites.").

comprehensive international treaty related to undersea cables should also get underway.

The United States, given the transition to a new presidential administration, is well suited to lead on efforts to reform domestic laws related to undersea cables and respond to attackers and commercial actors. The Biden Administration must recognize the centrality of the undersea cable system to America's national security and economy; foreign actors have already come to that realization and are ready to exploit the nation's vulnerabilities.

Testimony by Alexander Botting

Before the

United States House of Representatives
Homeland Security Committee
Cybersecurity & Infrastructure Protection and Transportation & Maritime Security Subcommittees

Hearing on the topic of

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

OPENING REMARKS

Chairman Ogles, Ranking Member Swalwell, distinguished members of the Subcommittee, thank you for the invitation to appear before you today to discuss the critical issue of subsea cable infrastructure security.

My name is Alex Botting and I serve as Senior Director for Global Security & Technology Strategy at Venable LLP and as a Global Fellow at NYU's Wahba Institute for Strategic Competition. For the past decade, I've worked on issues at the intersection of digital technology, telecommunications and security – promoting policies that will make foundational digital technologies more secure.

Over the past two years, I've devoted considerable time to the issue of subsea cable security and recently authored a whitepaper on the topic entitled *Shoring Up Subsea Security*. My testimony incorporates the key findings and recommendations from that whitepaper.

If I could leave you with just two takeaways from today's hearing, they would be:

1. Redundancy is resilience. If cables are abundant and repairs are swift, the impact of any incident is limited. This, in turn, significantly reduces the incentive for our adversaries to engage in sabotage. Accordingly, we should pursue more efficient and transparent approvals processes for laying and repairing subsea cables, while of course maintaining high security standards.

2. Our investigations into disruptions to subsea cables are insufficient. Roughly 70% of subsea cable disruptions are caused by human activity. Yet, in almost all cases we fail to investigate negligence or malicious intent. If we believe that our adversaries may intend to engage in

sabotage, we must develop the means to distinguish between accidental and intentional disruption and proactively investigate human-induced disruptions.

The following testimony provides recommendations for the U.S. Government across three areas: enhancing the resilience of the global subsea cable ecosystem; ensuring the security of individual submarine cables against known threats; and implementing appropriate legal and institutional frameworks.

The implementation of some will be led by U.S. government agencies which fall outside of this Committee's jurisdiction. I'd like to draw your attention to three specific recommendations which the Department of Homeland Security (DHS) would be well-positioned to lead as a member of Team Telecom and the Sector Risk Management Agency for Communications, IT and Maritime Transportation.

- DHS should serve as a single point of contact to centralize information and serve as an initial liaison for government agencies, and private parties regarding existing and planned submarine cables.
- DHS should collaborate with industry to conduct a comprehensive mapping of the submarine cable supply chain to identify potential choke points or areas of reliance on untrusted vendors and ensure that appropriate risk mitigations are in place.
- DHS should manage a proactive two-way intelligence sharing mechanism with trusted cable developers and vendors to pre-empt potential attacks, and support the evidentiary body needed to prosecute criminal activity.

As we seek to insulate ourselves against threats from our adversaries, we should note that the continental United States is quite well-protected against a major subsea cable outage. We are served by almost 100 subsea cable landings, more than any other country. These cables land at diverse points on the East and West coasts, markedly reducing the risk that a single incident inhibits our access to the global internet. Moreover, in contrast to the Radio Access Network market, trusted vendors are the dominant players.

Because subsea cables are part of a globally connected ecosystem, and U.S. force projection depends upon deployments beyond our shores, it's critical that we work with international partners to promote the implementation of policy best practices, and enhance one another's understanding of the threat environment.

Subsea cables underpin the global internet and, in an era where critical infrastructure is increasingly networked, they are foundational to the operation of critical services upon which we rely every day. Given their criticality, we should not take today's security for granted. It is essential that we stay ahead of emerging security threats and resilient against incidents. Doing so will require robust multi-stakeholder and multi-country cooperation.

WHY SUBSEA CABLES ARE ESSENTIAL

There are few technologies more foundational to the modern economy than subsea cables. As of 2024, five and a half billion people had access to the global internet and the associated economic benefits. A network of 597 subsea fiber optic cables[i], largely operated by the private sector, enable them to do so by carrying more than 95% of intercontinental data traffic.[ii] Beyond use by individuals, subsea cables are essential to the operation of critical sectors including financial services, defense, and telecommunications.

Today the most advanced cables can transmit more than 350 terabits per second along the ocean floor, equivalent to "the entire digitized Library of Congress three times every second."[iii] This achievement is driven by investments in technological innovation and the global economy's insatiable demand for data, which has risen from roughly 100 gigabytes of traffic per day in 1992,[iv] to an estimated 495.89 million terabytes per day in 2025.[v]

With advanced-AI workloads introducing new demands for the movement of data, global demand will continue to grow significantly in the years ahead. There is no feasible pathway to meet this demand that does not include significant investment in subsea cable infrastructure.

The rapid deployment of Low Earth Orbit (LEO) satellites is an impressive technological feat, but as of 2024 the combined capacity of every SpaceX satellite was a little under 350 terabits per second.[vi] A single cutting-edge cable such as the "Grace Hopper", meanwhile, can transmit 352 terabits of data per second.[vii] As modern societies come to depend ever more on data and computing capabilities, the "cloud under the sea" is indispensable to the operation of a modern economy.

Given the critical function that they fulfill, submarine cables should be, and in many countries are, categorized as critical infrastructure themselves. This designation affords them additional attention from industry and government stakeholders to ensure their ongoing security and resilience.

THE THREAT ENVIRONMENT FOR SUBSEA CABLE INFRASTRUCTURE

Owing to the vast distances that they cover, subsea cables are inherently vulnerable to accidental damage, natural disasters, or malicious interference. Across the 597 cables in operation today, roughly 150-200 incidents impact their operations during a typical year, according to the International Cable Protection Committee (ICPC).[viii]

Recent disruptions to cables and rising geopolitical tensions have spurred governments to intensify scrutiny of submarine cable accidents. Public reporting that China has developed a cable-cutting device capable of severing highly fortified cables at a depth of 4,000 meters has amplified concerns.[ix] As has the discovery of "Project Harmony", a seabed sensor network

established by Russia.[x] Concerns have been amplified further by high-profile instances of cable disruptions in the Baltic Sea[xi] and the Taiwan Strait[xii], the latter of which saw more cable disruptions in January 2025 than in either 2023 or 2024.

In an era of deep mistrust, it is easy to overstate the extent of exploitation occurring today. Yet, while sabotage may occur, it is in all likelihood rare. According to ICPC, the vast majority of incidents – approximately 70% in any given year – are caused by physical damage from fishing activity or anchoring.[xiii] The remainder result from natural events (such as storms or earthquakes), abrasion, or internal system failures. These incidents are longstanding and typically well-managed.

Beyond cuts to subsea cables, there is a theoretical risk of data interception on a subsea cable. As noted on pages 12-13, at this time this is unlikely to be implemented in practice without detection. Nevertheless, while the risk of exploitation is low today, public and private sector stakeholders should continue to assess the capabilities of adversaries, informed by government intelligence where possible, and adjust their assessment of the risk accordingly.

Finally, there is the risk that untrusted vendors in subsea cable supply chains could compromise the confidentiality of data, or availability of networks. This issue parallels the challenges faced during the rollout of 5G communications when Chinese companies like Huawei and ZTE leveraged government subsidies to dominate the telecommunications market, especially in emerging economies.

China continues to lead in advanced optical communications research, producing 37.7% of the field's research compared to just 12.8% from the U.S., underscoring the urgency for democratic nations to restrict untrusted vendors from developing and controlling optical core network infrastructure.[xiv] Today, trusted vendors maintain a technological advantage and a leading market position, but we should not take this for granted.

PROMOTING RESILIENCE IN THE ECOSYSTEM

Cable Redundancy

Building redundancy into submarine cable routes is vital for the resilience and reliability of global communications. If cables are abundant and repairs are swift, cuts will have limited practical impact. This significantly reduces the incentive for our adversaries to engage in sabotage.

To enhance resilience, companies design networks such that each node connects to at least two others, allowing traffic rerouting. They also seek to ensure that the supply of capacity stays ahead of demand at both a local and global level. The building of new cables is resource intensive, however, often requiring hundreds of millions of dollars in investment.

Cumbersome and opaque permitting and licensing regimes add to expense and extend the timeline for deployments, discouraging investment. In the U.S., permitting timelines have stretched from under a year to over three years, involving up to eleven agencies with overlapping mandates for environmental, historical, and national security concerns. [xv] Moreover, national security reviews are often slow and can result in the denial of a landing license after years of investment, where government guidance earlier in the process could have redirected cable operators to more palatable routes or partners.

This lack of coordination, transparency, and predictability creates uncertainty, deters investors, and can even increase vulnerability through geographic clustering. Enhancing transparency with trusted private sector partners and streamlining permitting and licensing processes, while maintaining security standards, is thus critical to enhancing resilience.

In instances where laying additional subsea cables isn't commercially feasible, such as in remote islands, governments and development partners should explore alternative financing mechanisms or satellite-based alternatives to subsea cables to ensure resilience against single points of failure.

Recommendations

1. The U.S. Government should ensure that permit requirements for the installation and repair of submarine cables are transparent and establish clear timeframes for approvals that are as short as possible, without undermining security.
2. The U.S. Government should enhance clarity and predictability of rules, partners, and geographies that will factor into approvals decisions, and promote transparency between national security agencies and submarine cable developers about security risks.
3. The U.S. Government should establish and communicate clear security and resilience requirements which are aligned with international standards and harmonized with national security review processes.

Effective route planning

At a global level, route diversity is a common best practice as it allows data to reroute around damaged segments, reducing disruption and deterring sabotage. Within a given country's EEZ, however, governments and industry may decide between diversifying cable routes and landings or concentrating them in Cable Protection Zones (CPZs).[xvi]

While diversification minimizes the impact of an individual incident, it's not always feasible for countries with limited coastline, crowded marine environments, or facing hostile maritime disputes, such as the South China Sea. Where diversification isn't possible, Cable Protection Zones (CPZs) can safeguard concentrated routes by restricting anchoring and fishing. Governments must, however, enforce protection measures and penalize violations to reduce the risk that one event could damage multiple systems.

Ultimately, the U.S.'s current approach of diversifying cable routes and landings is the most appropriate for its circumstances.

Recommendations

4. The U.S. Government should foster commercial and regulatory conditions that support the development of diverse submarine cable landing sites and pathways, including streamlining permitting approvals processes.
5. The U.S. Government should establish regulatory frameworks that embed submarine cable considerations into marine spatial planning processes, ensuring early-stage coordination with submarine cable stakeholders during the planning and development of other marine activities.
6. The U.S. Government should coordinate with trusted international partners to harmonize (to the extent possible) licensing and permitting requirements.

Facilitating timely cable repairs

Fast, efficient repairs limit the disruption from security incidents, yet cabotage laws, permitting delays, customs fees, high costs, and limited repair vessels slow recovery efforts on many cables today. Although most systems can be repaired within two weeks, recent data show average repair times now go beyond that, owing to delays caused by permitting, weather, or backlogs.[xvii]

The imposition of cabotage requirements, which mandate the use of locally built and crewed vessels, is a problem at a global level. These rules increase costs, delay urgent repairs, and conflict with international law under UNCLOS, which affirms freedom to maintain cables in international and exclusive economic zones.[xviii]

Likewise, mandatory port calls and customs duties add unnecessary delays and costs. Streamlining entry procedures and eliminating taxes and tariffs on repair operations accelerates service restoration. Establishing free ports with bonded storage facilities further reduces friction, allowing secure, duty-free storage of repair materials until needed.

Recommendations:

7. The U.S. Government should actively engage with international partners to address barriers to cable repair, which not only impair local capacity but also undermine the resilience of the global ecosystem. This includes:

    7.1 Refraining from classifying submarine cable installation and repair activities as cabotage and from imposing cabotage or crewing restrictions on repair vessels.

    7.2 Eliminating port entry requirements for cable ships engaged in installation or repair operations.

7.3 Avoid imposing customs duties, taxes, and fees on submarine cable installation and repair activities, by enabling the establishment of Free Ports with bonded storage facilities at vessel base ports to facilitate deployment and expedite repairs.

Global repair ship capacity

The global fleet of repair ships is limited in size and distributed across the globe, which can cause delays in remote or high-traffic areas. Although most repair operations are handled by trusted entities, we do rely on a narrow vendor base that includes as least one untrusted vendor – China's S.B. Submarine Systems (SBSS) – which participates in repair efforts in the North Pacific region.[xix]

The U.S. established the Cable Security Fleet (CSF) in 2021, to ensure rapid response and repair capacity during emergencies. While this program strengthens U.S. capabilities, each new repair ship costs over $100 million, requiring a long-term commitment.[xx] Governments should ensure private sector involvement in developing public policy initiatives to boost repair, to ensure that they do not inadvertently reduce incentives for private industry to invest in and maintain commercial repair capacity.

Instead, the U.S. Department of Homeland Security should collaborate with industry to develop an emergency response capability, designed for targeted interventions in exceptional circumstances, such as major natural disasters or acts of sabotage.

Recommendations:

8. The U.S. Government should co-develop a strategy with industry for emergency cable repair capacity, to enable additional government resources to be deployed in the event of a widespread disruption to cables.
9. The U.S. Government should streamline regulatory frameworks to ensure efficient cable repair, while maintaining security and transparency. This includes improving permitting and liability regimes.

Secure and trusted supply chains

Resilience is dependent upon access to uninterrupted provision of the trusted components necessary for laying, repairing, and maintaining submarine cables. Today, global repair and installation capacity is concentrated among a few providers, leaving little room for expansion and creating potential chokepoints. Because no single country has enough repair demand to sustain its own market, operators rely on regional maintenance agreements to share ships and resources.

Within subsea cable infrastructure supply chains, potential market dominance by untrusted vendors, especially Chinese state-backed firms, poses a strategic risk. As seen during the 5G rollout with Huawei and ZTE, such control can enable authoritarian influence over global communications.

While trusted vendors lead the market today, China's leadership in optical communications research, producing nearly 38% of global output versus 13% from the U.S., underscores the need for the U.S. to invest in innovation, strengthen domestic R&D, and avoid dependency on Chinese vendors.[xxi] Collaboration between cable operators and governments to mitigate these risks is critical.

Recommendations:

10. DHS should collaborate with industry to conduct a comprehensive mapping of the submarine cable supply chain to identify potential choke points or areas of reliance on untrusted vendors and ensure that appropriate risk mitigations are in place.
11. The U.S. Government should maintain a published list of untrusted providers which will guide industry in the development of their supply chain partnerships.
12. The U.S. Government and trusted industry partners should cooperate on sharing risk and incident data to identify protection gaps, enhance resilience, and detect and prevent malicious activities by state and non-state actors.

ENHANCING THE SECURITY OF CABLE INFRASTRUCTURE

Submarine cables are engineered to withstand extreme underwater conditions, protected by multiple layers of insulation and armoring. While they rest along the seabed in deeper waters, they are typically buried 0.5-3 meters deep when at less than 1500 meters to protect against damage.[xxii] Despite these measures, cables remain vulnerable to natural, accidental, and intentional harm.

Events such as earthquakes, volcanic eruptions, tsunamis, and underwater landslides occasionally damage cables, though less frequently than human activity. The most prevalent cause of disruption, however, is human disruption caused by fishing and anchoring, which accounts for roughly 70% of cable breaks annually.[xxiii]

Several mitigations are available and are being utilized to address these risks, particularly those related to accidental and intentional human activities. The most obvious measure is armoring cables for tensile and impact resistance.

Beyond physical reinforcement, Automated Identification Systems (AIS) or Vessel Monitoring Systems (VMS) can be used to provide real-time alerts regarding vessel movements, which facilitates better cable protection.[xxiv] It also aids the investigation of incidents after they occur.

Recommendations:

13. Industry should continue to armor cables deployed shallower than 1500 meters.
14. The U.S. Government should ensure the use of AIS tracking devices by vessels is mandatory in national law and enforce its use in accordance with IMO regulations.
15. Governments should explore making the use of VMS tracking mandatory within their EEZ to enhance visibility of activity near submarine cables, and enforcement against negligent activities.

Physical Security of Landing Stations

Of the world's 1.5 million kilometers of submarine fiber-optic cables, all connect to land through roughly 1,400 Cable Landing Stations (CLS). These shoreline facilities link subsea cables to terrestrial infrastructure – such as fiber-optic networks and satellites – that carry data to users and data centers. Like other critical infrastructure, CLS facilities face risks from natural hazards such as hurricanes, wildfires, and earthquakes, as well as intentional threats from malicious actors. A 2017 U.S. government report identified landing stations as "the most accessible and impact-rich targets"[xxv] within global communications systems.

While internet traffic can often be rerouted through other terrestrial or subsea pathways, damage to a major CLS that connects multiple cables can still cause widespread outages.[xxvi] For this reason, network designers build redundancy by diversifying cable routes and landing points.

Protection of CLS sites is relatively comprehensive due to their fixed locations and clearer jurisdictional control. Standard safeguards include physical security measures—such as surveillance, access control, and intrusion detection—as well as resilience planning for energy supply and disaster impacts. Together, these practices form a mature framework for protecting critical coastal infrastructure that underpins global connectivity.

Recommendations:

16. The U.S. Government should work with industry to define clear security best practices for cable landing stations and work cooperatively to implement risk-based measures that enhance the overall resilience and security.

Interception of Data on Cables

Given the technical complexity of this type of espionage, the theoretical risk is unlikely to be implemented effectively at this time for three reasons: it requires enormous technical and financial resources, the sheer data volume makes useful extraction nearly impossible, and any physical interference will create detectable anomalies in the cable's performance.

Interfering with active cables post-deployment, however, is highly complex and limited to nation-states with advanced resources. There are reasonable concerns about Chinese-operated vessels like SBSS[xxvii] and research ships such as *Tan Suo Yi Hao*[xxviii] conducting suspicious activities near major cable routes. Yet much of the data that traverses networks today is encrypted. Even attempts to pursue a "harvest now, decrypt later"[xxix] strategy would require sufficient storage to retain up to 352 TBPS of data, overwhelming the resources of even the most well-resourced actors and creating a "needle in a haystack" problem. Moreover, any attempts to tamper with the cable undersea would likely create anomalies in the light passing through the cable, which would be captured by the modems.

To mitigate future threats, data owners should implement strong encryption in transit and plan migration to post-quantum cryptography. Ultimately, however, given the vast resources required and without a clear path to generating usable information, the risk associated with cable 'tapping' remains very low and the efforts of adversarial nation states are likely to be directed toward more accessible targets.

Vulnerabilities could, however, be introduced during manufacturing or storage. Cable components kept in depots, such as China's Wujing Depot, may face higher tampering risks due to weaker security controls. While there is currently limited public evidence of exploitation, the long-term storage of components in jurisdictions of strategic concern warrants continued vigilance and mitigation of risks.

<u>Recommendations:</u>

17. Industry owners of data should continue to implement comprehensive data risk mitigation frameworks including, where feasible, encrypting data in transit.
18. The U.S. Government and industry owners of data should ensure timely transition to quantum-resistant algorithms when encrypting sensitive data.
19. DHS should work with industry to map potential supply chain risks, to include those to the repair supply chain.

Emerging Detection Capabilities

One emerging technology – fiber sensing – can also play a role in improving real-time incident detection. Fiber sensing leverages the optical transmission technology used by modern cables to

send information between endpoints. The oscillation direction of the electric field, known as the State of Polarization (SOP), changes as the light propagates. The SOP is sensitive to external stimuli, such as the pressure and physical movements experienced by the fiber, enabling fiber sensing technologies integrated into modems to monitor and detect variations to the SOP.[xxx]

By analyzing these changes, operators can gain valuable insights into the physical movements or disturbances affecting the cable, enabling real-time detection of tampering or damage. Beyond detecting damage to cables after they have gone offline, fiber sensing can provide insights into underwater activity in the vicinity of submarine cables. This could improve investigations, support attribution of incidents, and increase accountability, thereby enhancing deterrence.

Additionally, fiber sensing can serve as an early warning system for natural hazards. For example, changes in the SOP of a particular submarine cable caused by an underwater earthquake could provide information to early warnings of tsunamis, allowing governments to mitigate harms to populated areas.

While fiber sensing may enhance situational awareness and cable protection, however, its deployment raises important legal considerations. Adding fiber sensing to a cable may reclassify it from a purely telecommunications cable to a measurement device. To enable the widespread use of fiber sensing on cables crossing such jurisdictions, further clarification of UNCLOS provisions will be necessary to ensure continued compliance with international law.

Recommendations:

20. The U.S. Government and industry should continue to invest in research and development (R&D) to advance fiber sensing capabilities and establish clear guidance on the approvals process for, and use of, fiber sensing solutions.

21. The U.S. Government and industry should explore potential information sharing agreements to leverage real-time data regarding imminent natural disasters.

IMPLEMENTING LEGAL & INSTITUTIONAL FRAMEWORKS

Domestic Legal Frameworks

Legal and institutional frameworks play a critical role in reinforcing risk mitigation and deterrence. If designed effectively, they will catalyze security and resilience efforts by promoting awareness of risks, enhancing multi-stakeholder coordination, reducing instances of unintentional disruption, and adequately deterring acts of aggression.

Governments can play a constructive role firstly by enhancing transparency around national security priorities. For example, publishing clear guidance on high-risk countries, prohibited

equipment, and entities and countries of concern would help infrastructure operators make informed decisions.

Secondly, by implementing national obligations under 1884 and UNCLOS. Article II of the former states that it's "a punishable offence to break or injure a submarine cable, willfully or by culpable negligence, in such a manner as might interrupt or obstruct telegraphic communication."[xxxi] Article 113 of UNCLOS, meanwhile, requires countries to adopt laws to punish people or ships under its jurisdiction for damaging or breaking submarine cables on the high seas, whether "done willfully or through culpable negligence."[xxxii] Yet while on the surface this provides a robust enforcement framework, in reality it is enforced sporadically.

Thirdly, by enforcing IMO-required use of Automatic Identification Systems (AIS). AIS is required to be fitted on most large ships. Yet according to a recent study, enforcement is poor and "sanctions are not severe enough to act as deterrents."[xxxiii] Many vessels deactivate AIS to evade detection while illegally fishing in protected areas or to avoid revealing lucrative fishing areas to competitors.[xxxiv]

Finally, governments should ensure coordinated use of the territorial seabed. This can be done by mandating educational programs for maritime employees via local marine and fishing authorities, to ensure they are aware of key cable pathways, charting requirements, and measures to avoid accidental disruption.

Where fishing vessels are negligent in applying these measures, penalties should be enforced, even in cases of accidental disruption, to incentivize compliance. Due to the inherently cross border nature of this infrastructure, the U.S. should also promote their implementation by foreign governments.

Recommendations:

22. The U.S. Government should implement national obligations under 1884 and UNCLOS, where applicable.
23. The U.S. Government should ensure IMO-required use of Automatic Identification System (AIS) tracking.
24. The U.S. Government should ensure that charting authorities update nautical charts regularly; ensure implementation of the amended IHO Resolution 4/1967; and mandate educational programs for employees of maritime vessels.
25. The U.S. Government should establish and rigorously enforce penalties for the disruption of cables through negligence and encourage international partners to do the same.

International Collaboration

Effective deterrence necessitates the ability to monitor, intercept, and penalize vessels that may cause disruption within the territorial sea. The cable ecosystem covers such vast territory, however, that it would require an unfeasible number of resources for countries to patrol the high seas individually.

The U.S. Government should work with international partners, leverage existing security mechanisms such as NATO or the Quad, to establish a multilateral mechanism for conducting patrols, focused on high-risk areas. These include regions that are experiencing acute geopolitical instability (e.g. Baltic Sea), have cables that are more physically exposed (e.g. Red Sea), or are key fulcrums for the global ecosystem (e.g. Straits of Malacca).

Supporting these efforts, governments should establish or expand mechanisms for intelligence-sharing with trusted partners to pre-empt potential attacks, adapt patrol activities accordingly, and support the evidentiary body needed to convict saboteurs. While the private sector has proven itself adept at ensuring continuity of service during past outages, only governments can conduct the kind of operational activities needed to deter acts of international negligence or aggression.

Beyond operational collaboration, there are critical gaps in the existing international legal architecture for submarine cables. Even if likeminded countries enforce their obligations under 1884 and UNCLOS at a domestic level, state actors can opt not to impose penalties on ships bearing their flag that engage in sabotage on the High Seas. As recent disruptions in the Baltic Sea and Taiwan Strait have demonstrated, existing legal frameworks in many countries make it highly challenging to intercept, investigate, or prosecute security incidents, even where governments suspect intentional foul play.[xxxv] Whether these incidents are deemed to be accidental or intentional acts of sabotage, our inability to address acts of sabotage if and when they occur inhibits our ability to deter such behavior.

Recommendations:

26. The U.S. Government should leverage existing security cooperation agreements to conduct patrols in high-risk areas and share intelligence about potential threats.
27. DHS should manage a proactive two-way intelligence sharing mechanism with trusted cable developers and vendors to pre-empt potential attacks, and support the evidentiary body needed to prosecute criminal activity.

Multi-Stakeholder Coordination

Government and industry have a shared interest in promoting the security and resilience of submarine cable infrastructure, yet mechanisms for public-private coordination are limited. To remedy this, governments should take steps to formalize their private sector engagement. These

efforts should initially focus on: establishing a Single Point of Contact (SPOC) for private sector engagement; establishing two-way threat intelligence sharing with private stakeholders; and enhancing transparency around trusted vendors.

In most governments, multiple agencies have responsibility for some aspect of submarine cable resilience. Their remit may cut across environmental, commercial, or security considerations and their authorities may encompass new cable approvals, repair activities, or critical infrastructure protection. Governments can reduce inefficiencies, while meeting desired security outcomes, by appointing a SPOC responsible for engaging companies as they navigate regulatory processes. Their role would not prevent direct engagement with individual agencies. Rather, this office would serve as the primary external liaison to private entities and internally drive maximum efficiency and transparency of the process.

The important role of private companies in deploying, maintaining, and securing these assets also necessitates multi-stakeholder threat intelligence sharing. This enables public and private organizations to benefit from information, analysis, and context that they would not be privy to individually and provides an early warning system against potential threats. Beyond direct information about tactics, techniques and indicators of compromise, this creates a common understanding of the threat environment and what steps need to be taken to mitigate risks.

Untrusted vendors have been successful in winning contracts for subsea cable infrastructure. While this is less acute than in Radio Access Networks, organizations like HMN continue to leverage significant Chinese government subsidies to undercut bids from competitors by up to a third.[xxxvi] While matching China's bids dollar-for-dollar is not a feasible long-term solution, likeminded governments can reduce the strategic advantage of untrusted vendors by publishing clear guidance on high-risk equipment, entities of concern, and trusted suppliers. This transparency would help infrastructure operators make informed procurement decisions early in the planning process and ensure alignment with national security objectives. Such guidance can also deter the use of untrusted vendors by signaling potential risks, while supporting trusted vendors in producing competitive, security-enhancing bids.

Recommendations:

28. DHS should serve as a single point of contact to centralize information and serve as an initial liaison for government agencies, and private parties regarding existing and planned submarine cables.

29. The U.S. Government should publish clear guidance on high-risk equipment, entities and countries of concern, and trusted suppliers.

30. The U.S. Government should establish formal 1.5 track dialogues with trusted industry partners through existing regional and security groupings, such as the Quad and NATO, to support aligned approaches to submarine cable security and resilience.

[i] TeleGeography, Submarine Cable Map 2025, https://submarine-cable-map-2025.telegeography.com/.
[ii] TeleGeography, "Submarine Cable Frequently Asked Questions," (last accessed Nov. 17, 2025). www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.
[iii] Chris Ciauri, "The Dunant subsea cable, connecting the US and mainland Europe, is ready for service," Google, Feb.3, 2021, cloud.google.com/blog/products/infrastructure/googles-dunant-subsea-cable-is-now-ready-for-service.
[iv] UNCTAD, *Global efforts needed to spread digital economy benefits https://unctad.org/news/global-efforts-needed-spread-digital-economy-benefits-un-report-says*
[v] https://www.statista.com/statistics/871513/worldwide-data-created/
[vi] Universe Space Tech, "SpaceX presents Starlink V3 satellites with 1 Tbps speeds," Jan 7, 2025, https://universemagazine.com/en/spacex-presents-starlink-v3-satellites-with-1-tbps-speeds/?srsltid=AfmBOor-h6nkfdYkNrl-hH5gyGg_XH6PFBeM00ZrWa_FyOtc4ecNdVBE.
[vii] Federal Communications Commission, Report No. SCL-00352 Actions Taken Under Cable Landing License Act, Jan. 14, 2022, https://docs.fcc.gov/public/attachments/DA-22-44A1_Rcd.pdf#:~:text=Cable%20Design%20and%20Capacity:%20Grace%20Hopper%20will,system%20design%20capacity%20of%20approximately%20352%20Tbps..
[viii] International Cable Protection Committee (ICPC), Media Enquiries & Frequently Asked Question, May 16, 2025, https://www.iscpc.org/news/media-enquiries/.
[ix] The Diplomat, "China's new deep-sea cutting tool exposes vulnerability of undersea cables," April 16, 2025, https://thediplomat.com/2025/04/chinas-new-deep-sea-cutting-tool-exposes-vulnerability-of-undersea-cables/.
[x] International Consortium of Investigative Journalists, "Russia secretly acquired Western technology to protect its nuclear submarine fleet," Oct. 23, 2025, https://www.icij.org/investigations/russia-archive/russia-secretly-acquired-western-technology-to-protect-its-nuclear-submarine-fleet/.
[xi] Associated Press, "Sweden seizes vessel suspected of 'sabotage' after undersea data cable rupture in Baltic Sea," Jan. 27, 2025, https://apnews.com/article/latvia-denmark-underwater-cable-damage-investigation-63da5ef0d577bca12bbe118d527d3a14.
[xii] ABC News, "Taiwan detains China-linked cargo ship after undersea cable disconnected," Feb. 25, 2025, https://www.abc.net.au/news/2025-02-25/taiwan-detains-china-linked-ship-after-undersea-cable-incident/104981932.
[xiii] ICPC, "Charting submarine cables is critical for maritime safety & infrastructure protection," June 25, 2025, https://www.iscpc.org/publications/icpc-viewpoints/charting-submarine-cables-is-critical-for-maritime-safety-and-infrastructure-protection/.
[xiv] Australian Strategic Policy Institute (ASPI), Critical Technology Tracker, March 1, 2023, https://www.aspi.org.au/report/critical-technology-tracker/#6a5a9bb3-c58e-4909-85f4-78bd875c0a80-link.
[xv] Department of Homeland Security (DHS), Priorities for DHS Engagement on Subsea Cable Security & Resilience, Dec. 18, 2024, www.dhs.gov/publication/priorities-dhs-engagement-subsea-cable-security-resilience.
[xvi] International Cable Protection Committee, Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables Version 1.2, (last accessed Nov. 17, 2025), pg. 3, https://www.iscpc.org/documents/?id=3733.
[xvii] Recorded Future, Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity, July 17, 2025, https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-2025-0717.pdf.
[xviii] ICPC, Government Best Practices, pg. 9
[xix] The Wall Street Journal, "U.S. Fears Undersea Cables are Vulnerable to Espionage from Chinese Repair Ships," May 19, 2024, https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320?gaa_at=eafs&gaa_n=AWEtsqfyEGd0IiscfyyxW9hIWjo81A0KIhm6vclhvq9qX5Dqz5-zFdPBaDY037Uqm0Y%3D&gaa_ts=691b909c&gaa_sig=pdns4KMa_RE6jXl2cxwWTF-glzZzsrrZRQAdpCfsf6n2ZsYAsMqHUR5gu_R7fatAnf8Qg4vv_GmY-H4O3q3gtw%3D%3D.
[xx] Center for Strategic & International Studies (CSIS), Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition, August 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.
[xxi] Australian Strategic Policy Institute (ASPI), Critical Technology Tracker, March 1, 2023, https://www.aspi.org.au/report/critical-technology-tracker/#6a5a9bb3-c58e-4909-85f4-78bd875c0a80-link.
[xxii] ICPC, Government Best Practices, pg. 2

[xxiii] ICPC, Government Best Practices, pg. 1
[xxiv] ICPC, Government Best Practices, pg. 2
[xxv] CRS, *Protection of Undersea Telecommunication Cables*, pg. 6.
[xxvi] Data Center Dynamics, "What is a cable landing station?"
[xxvii] Daniel Runde et. al., *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, CSIS, Aug. 2024, pg. 4., www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.
[xxviii] Samantha Dick and Stephen Dziedzic, "Dutton says Chinese research ship is collecting intelligence, mapping undersea cables," *ABC News,* Mar. 31, 2025, www.abc.net.au/news/2025-04-01/dutton-says-chinese-research-ship-mapping-undersea-cables/105122068.
[xxix] K. F. Hasan *et al*., *A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies,* IEEE Access, Feb. 16, 2024, pg. 23431
[xxx] Brian Lavallee, "Detecting Undersea Earthquakes with Cross-Industry Collaboration," *Ciena*, Feb. 22, 2024, https://www.ciena.com/insights/articles/2022/detecting-undersea-earthquakes-with-cross-industry-collaboration
[xxxi] *1884 Convention for the Protection of Submarine Telegraph Cables*, Mar. 14, 1884, p. 2, https://cil.nus.edu.sg/wp-content/uploads/2019/02/1884-Convention-for-the-Protection-of-Submarine-Telegraph - Cables-1.pdf
[xxxii] UN, *Convention on the Law of the Sea*, pg. 64
[xxxiii] Priyal Bunwaree, *The Illegality of Fishing Vessels 'Going Dark' and Methods of Deterrence*, Cambridge University Press, Jan. 11, 2023, pg. 191
[xxxiv] Oceana, "Avoiding Detection Global Case Studies."
[xxxv] Miranda Bryant, "Sweden says China denied request for prosecutors to board ship linked to severed cables," The *Guardian*, Dec. 23, 2024
[xxxvi] Joe Brock, "US and China wage war beneath the waves - over internet cables," *Reuters*, Mar. 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/