CSIS BRIEFS

Securing Asia's Subsea Network

U.S. Interests and Strategic Options

By Matthew P. Goodman and Matthew Wayland

APRIL 2022

THE ISSUE

More than 1 million kilometers of submarine cables traversing the ocean floor, each about as wide as a garden hose, transmit up to 99 percent of international data, underpinning global trade and communication. This vital digital infrastructure faces myriad threats, from earthquakes and typhoons to fishing nets and saboteurs. The United States derives significant advantages from its centrality in Asia's subsea cables, which contribute up to $169 billion to the U.S. economy annually and could benefit more U.S. workers and businesses as demand for digital products and services grows globally. But realizing those benefits will require the United States to step up its policy engagement on Asia's cable networks, which are changing with China's rise, the emergence of new regional hubs, and new transpacific routes designed to reduce risks and increase network resiliency.

U.S. INTERESTS

SUBSEA CABLES ARE INCREASINGLY VITAL

The United States derives significant benefits from its leading position in global subsea cable networks, which carry the vast majority of voice and internet traffic between continents. There are approximately **436 cables** in service around the world, and dozens of them land on U.S. coasts. These systems support a wide and growing range of U.S. economic activities and have become even more important to workers and businesses during the Covid-19 pandemic.[1]

The early stages of the pandemic led to a surge in internet traffic that subsea cables accommodated, accelerating the digitization of modern economies. Connected communities were able to adapt and even benefit from shifts to online work, education, healthcare, and other activities. Students and teachers moved their lessons online, physicians and patients embraced new applications for remote consultation and treatment, and businesses adopted new tools for meeting and collaborating virtually.

Digitalization will intensify with the arrival of 5G and the expansion of the Internet of Things, which will combine to unlock new possibilities in U.S. manufacturing. For example, the **auto industry** is using advanced sensors and real-time analytics to increase connectivity among vehicles, users, and their surroundings. **Leading manufacturers** are also using digitalization to improve logistics and production planning, allowing for greater visibility and control of their global supply chains. Tying these activities together across continents requires a resilient network of subsea cables and the free flow of data across them.

ECONOMIC IMPACT OF SUBSEA CABLES

The full contribution of subsea cables to the U.S. economy is difficult to precisely estimate.[2] As one industry expert put it, "Asking how important subsea cables are to a digitally-driven economy is like asking a fish how important water is." One very rough, back-of-the-envelope **method** is to consider the size of the U.S. digital economy, which hinges on internet traffic, and the percentages of

traffic that are routed internationally and carried by subsea cables. Doing so estimates the contribution of subsea cables to the U.S. economy at nearly $649 billion in 2019, or about 3 percent of U.S. GDP. Of that total, U.S. traffic routed through Asia is responsible for roughly $169 billion. Another telling indicator, depicted in Figure 1, is the contribution of U.S. digital exports, which rely on subsea cables and totaled $520 billion in 2020.

The U.S. financial sector, which is responsible for an estimated 6.7 million jobs and 7.5 percent of GDP, relies on subsea cables to support $10 trillion in daily transactions. Subsea cables also enhance the United States' attractiveness as a financial hub. On the other side of the Atlantic, the European Central Bank found that the large number of international cables landing in the United Kingdom increased the number of financial transactions in London by as much as one-third, strengthening its position as a **financial center**. With a high concentration of cable landings, New York and New Jersey enjoy similar network effects.

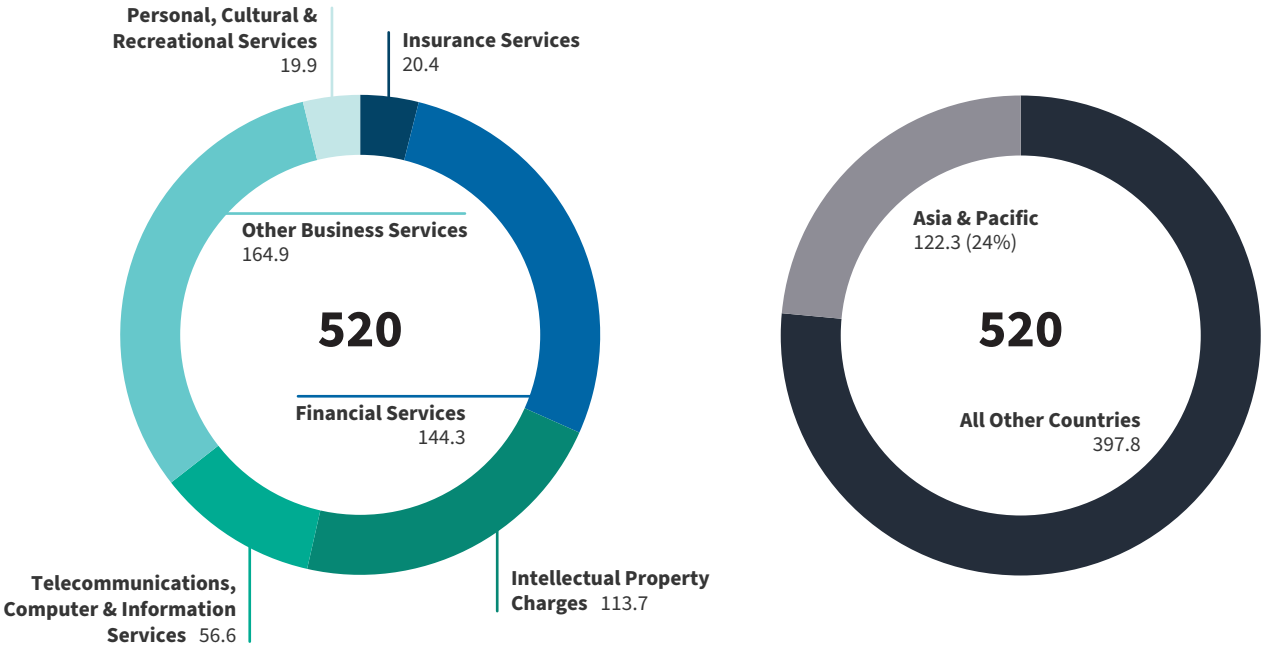
The rapid digitization of economies is also opening up new opportunities for U.S. businesses to export. Services trade—spanning advertising, insurance, travel arrangement and management, accounting, auditing, and consulting—is increasingly digital. In 2020, **U.S. digital exports** of services enabled by information and communications technology totaled nearly $520 billion, with the Asia-Pacific region accounting for $122 billion (23.4 percent). Digital exports comprised nearly 88 percent of the total U.S. service trade surplus in 2020.

Today, U.S. workers and businesses are just scratching the surface of digital export opportunities. Just **1 in every 20** U.S. providers of business services exports, compared to 1 in 4 U.S manufacturers. Increasing U.S. digital exports would help create more opportunities for U.S. workers in **professional and business services**, which is now estimated to be the second-largest employment sector in the United States (after healthcare) and is expected to grow to approximately 21 million jobs by 2024.

Digital export opportunities are particularly important for small and medium-sized enterprises (SMEs), firms with fewer than 500 employees. **SMEs** make up nearly 98 percent of the 300,000 U.S. companies that export and account for about one-third of total U.S. merchandise exports. But only 1 in every 100 of America's 30 million small businesses exports. In countries such as Germany and Switzerland, the share of SMEs that sell their products abroad is approximately 5 to 10 times larger on a per capita or per firm basis. If SMEs overcome these barriers to export, the U.S. Chamber of Commerce **estimates** they could create nearly 900,000 jobs.

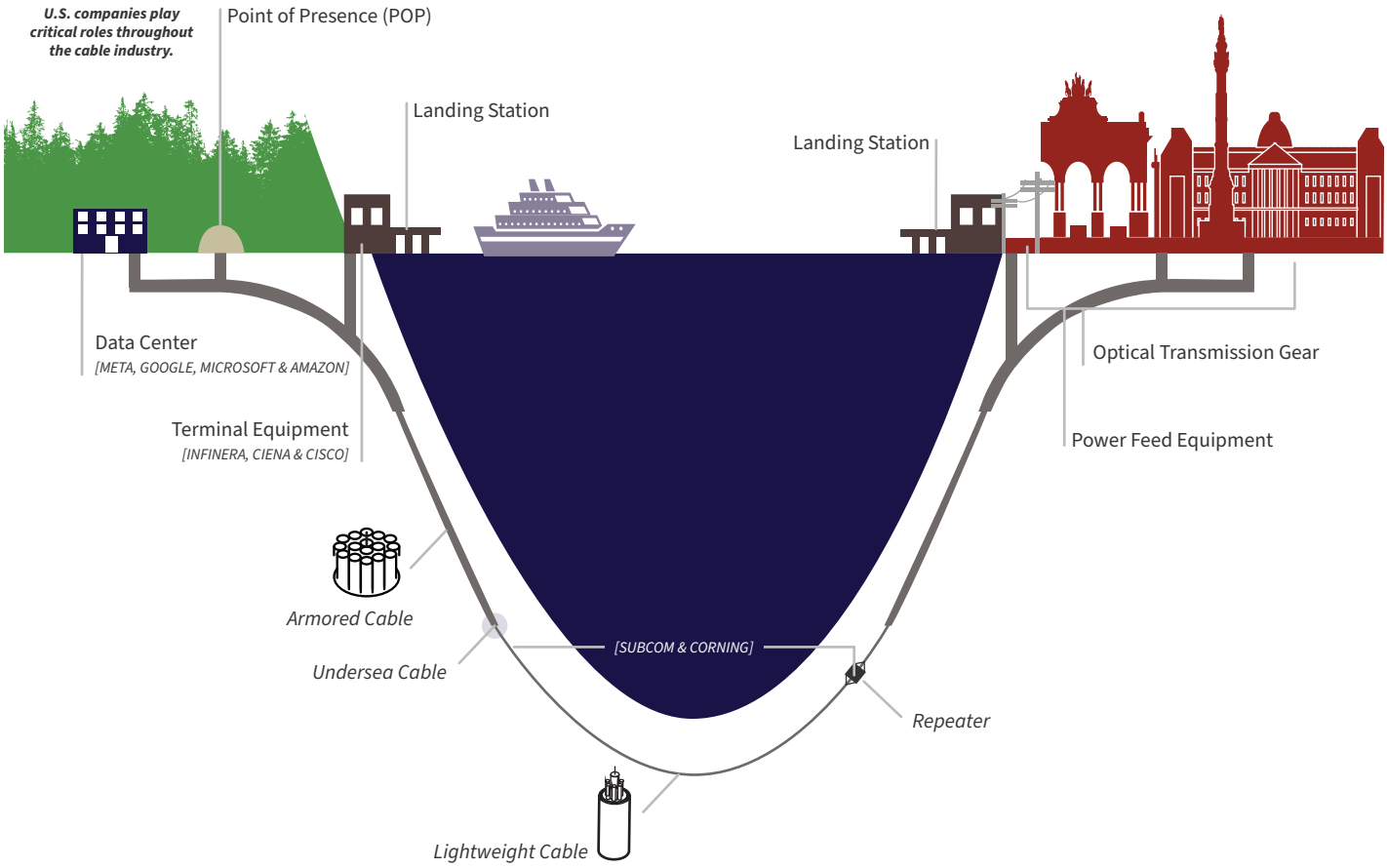
Figure 1: Subsea Cables Power U.S. Digital Exports

Digital Exports of Potential ICT-Enabled Services (in millions USD), 2020



Source: "International Data: International Transactions, International Services, and International Investment Position Tables," Bureau of Economic Analysis, https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4#reqid=62&step=9&isuri=1&6210=4.

Figure 2: Global Cables – Made in the United States



Source: Google; UK Cable Protection Committee; Alcatel-Lucent Submarine Network.

The United States is also home to leading providers of subsea components and related services, as illustrated in Figure 2. SubCom, based in New Jersey, **won** nearly a quarter of the global market for subsea cable manufacture and installation from 2015 to 2019. Technology company Corning has produced fiber for more than half of all worldwide cable systems manufactured and installed by SubCom and its competitors and employs about a thousand workers at its **manufacturing plant** in Wilmington, North Carolina. U.S. companies Infinera, Ciena, and Cisco are among the main suppliers for submarine line terminal equipment and key transmission components.

ASIA IS LEADING GLOBAL DEMAND

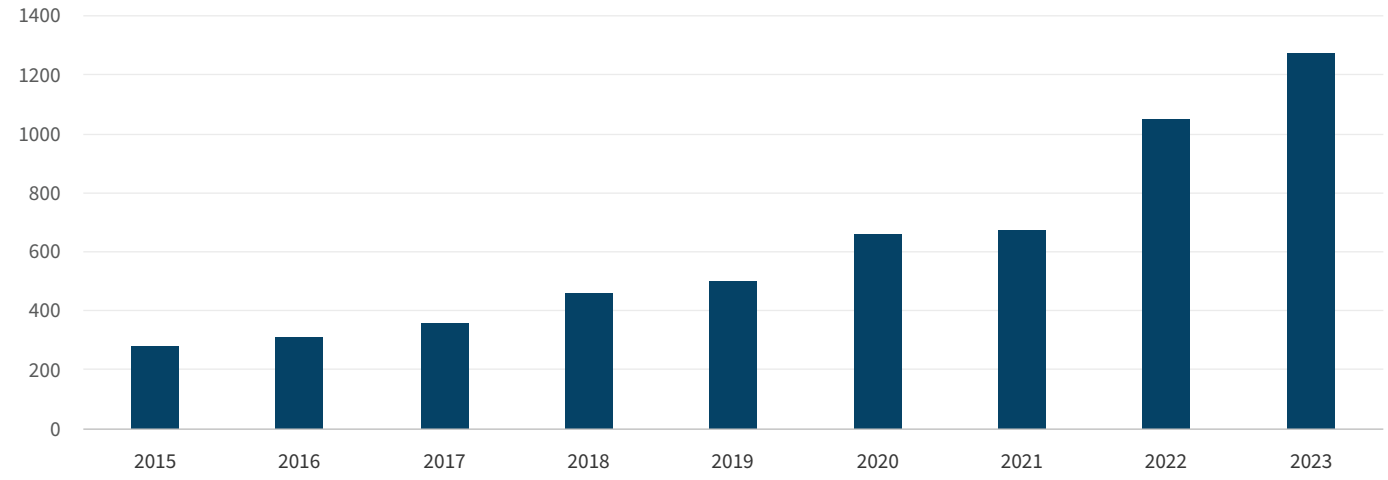
International bandwidth used by global networks more than doubled between 2017 and 2019, according to **TeleGeography**. Demand has been growing fastest on links connected to Asia, as shown in Figure 3, which experienced a compound annual growth rate of 56 percent between 2015 and 2019.

New investments are key to meeting this rising demand, considering the massive capital expenditures required to produce and lay cables. Between 2020 and 2022, $8.1 billion worth of cables were launched, with routes crossing the Pacific amounting to $2.3 billion of this total investment. One transpacific cable system was brought online each year between 2016 and 2020, and at least eight additional systems are planned through 2024.[3]

U.S. content providers are building much of this additional capacity to link their data centers and cloud networks. According to TeleGeography, **content providers** or "hyperscalers," led by Google, Meta, Microsoft, and Amazon, added capacity at a compound annual rate of at least 70 percent between 2015 and 2019 across six of the world's seven regions. As a result of this upsurge in capital expenditure, content providers have surpassed internet backbone providers to become the leading owners of subsea cable capacity.

Within Asia, Southeast Asia's digital economy is growing especially rapidly and, according to Google, could reach

Figure 3: Total Transpacific Capacity (Terabytes per second), 2015–2023



Source: Submarine Telecoms Forum, *Industry Report 2021/2022 Issue 10* (Sterling, Virginia: Submarine Telecoms Forum, 2021), 30, https://subtelforum.com/products/submarine-telecoms-industry-report/.

$1 trillion by **2030**. This is partially attributable to the Covid-19 pandemic, which accelerated the adoption and migration to digital channels such as mobile applications for financial services. Southeast Asia now has a total of 440 million internet users, with sectors such as e-commerce and food delivery powering growth. Twelve new **cable systems** are slated to begin service in Southeast Asia, Australia, and East Asia over the next three years.

EMERGING ISSUES

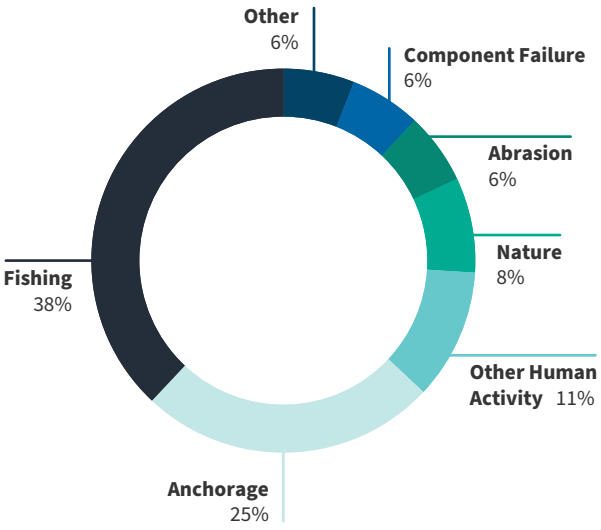
While the regional landscape is evolving, the most significant risks to subsea cable systems remain physical and environmental. Delivering transpacific systems requires navigating numerous technical challenges. Fishing activities and vessel anchors are the largest source of cable "faults" (operating events that will eventually require repair) globally each year. Seismic activity presents another risk. The Luzon Strait between the Philippines and Taiwan is traversed by more than 10 cable systems but is prone to earthquakes and turbidity currents due to its location on the Ring of Fire. Major earthquakes in **2006** and **2011** damaged multiple cables in the region and motivated cable planners to further diversify future routes.

Illustrating these threats to connectivity—and their serious consequences—is the South Pacific nation of Tonga. In February 2019, a **ship's anchor** severed the island's only subsea cable, knocking out internet and voice connectivity and throwing the tourism industry in disarray. In January 2022, a massive **volcanic eruption** damaged the same international cable and a domestic one, cutting Tonga off from the global internet for weeks, impairing domestic communications and complicating humanitarian relief efforts.

EVOLVING SECURITY THREATS

Although non-malicious activities such as fishing and vessel anchoring remain the principal source of cable damage, both the private sector and policymakers have expressed increasing concern about deliberate attacks on subsea cables in light of increasing geopolitical tensions. Among

Figure 4: Causes of Submarine Cable Faults



Source: Alan Mauldin, "Cable Breakage: When and How Cables Go Down," TeleGeography, May 3, 2017, https://blog.telegeography.com/what-happens-when-submarine-cables-break.

the foremost risks are that vital cables might be destroyed or disabled by adversaries. In recent years, **Russian activity** near undersea cables has raised alarm bells, including a **public warning** from the head of the United Kingdom's armed forces. State adversaries have **two primary means** to threaten cables: submarines and surface vessels that can deploy autonomous or manned submersibles. Nonstate actors have also found ways to disrupt cable systems, such as by **stealing** optical amplifiers.

Severing multiple cables could serve a number of targeted strategic purposes, from sowing economic disorder to cutting off critical government and public communications during the early stages of a conflict. Considerably more difficult than destroying the cables is tapping them to steal and then decrypt data, which is so technically challenging as to be practically impossible. Moreover, the widespread use of encryption, discussed further in the next section, makes "tapping" cables increasingly unlikely and unprofitable.

The other category of threat is cyber or network attacks on enabling information technology hardware and software—threats that are common to all electronic communications networks. Another posited concern is potential vulnerabilities in the network management systems that private companies use to manage data traffic passing through the cables. Because of the industry's ubiquitous use of encryption, attacking a network management system could have the same disruptive impact as a typical fiber cut but not expose data to theft.

GEOPOLITICAL RISKS ARE RESHAPING NETWORKS

Maritime and territorial disputes in the South China Sea (Figure 5), a major crossing point for subsea networks, have become an impediment to deploying transpacific cables. Since 2013, China has increased its land reclamation efforts, military base construction, and naval patrolling, including using its **maritime militia** in greater numbers to harass foreign ships. Companies laying cables through the South China Sea have to obtain permits for deployment and cable repairs from multiple countries including China, Taiwan, and other claimants. U.S. companies are vulnerable to Chinese regulators, who can prevent or significantly slow building and repair activities.

China's actions have also undercut Hong Kong's potential as a transpacific cable landing hub. In June 2020, a sweeping **national security law** went into effect that severely restricted Hong Kong's legal autonomy and formalized Chinese state security and intelligence services' jurisdiction over the island. Hong Kong, which ranks among the world's top metropolitan areas in international internet traffic, is likely to continue serving as the primary gateway to mainland China. But as new cables are planned, major investors are increasingly looking elsewhere.

Figure 5: South China Sea

Source: TeleGeography map adapted from Greg Poling, *The South China Sea in Focus: Clarifying the Limits of Maritime Dispute* (Washington, DC/Lanham, MD: CSIS/Rowman & Littlefield, 2013), https://www.csis.org/analysis/south-china-sea-focus. Reprinted with permission.

Cross-strait tensions are another source of risk. Taiwan is home to two hyperscale **data centers**, is connected to 15 submarine cables, and has more cables on the way, including the **Apricot** cable, which aims to connect Singapore, Japan, Guam, the Philippines, Taiwan, and Indonesia by 2024. To improve the resiliency of its networks, Taiwanese **domestic providers** have invested in strengthening their links with neighboring countries and participated in several international cable projects.

CHINA'S CABLES ARE EXPANDING WITH STATE SUPPORT

In recent years, Chinese companies have started investing heavily in owning and supplying subsea cables. In 2019, Hengtong Group, a private Chinese company that has cultivated government ties,

acquired Huawei Marine, the world's fourth-largest manufacturer of subsea cables, and rebranded it as HMN Technologies. Hengtong Group has won praise from the Chinese government for being a model of "**civil-military integration**," and a **press release** available only on the Chinese-language version of its website notes the company will "offer powerful support for the modernization of our country's national defense" and "advance into the international market."

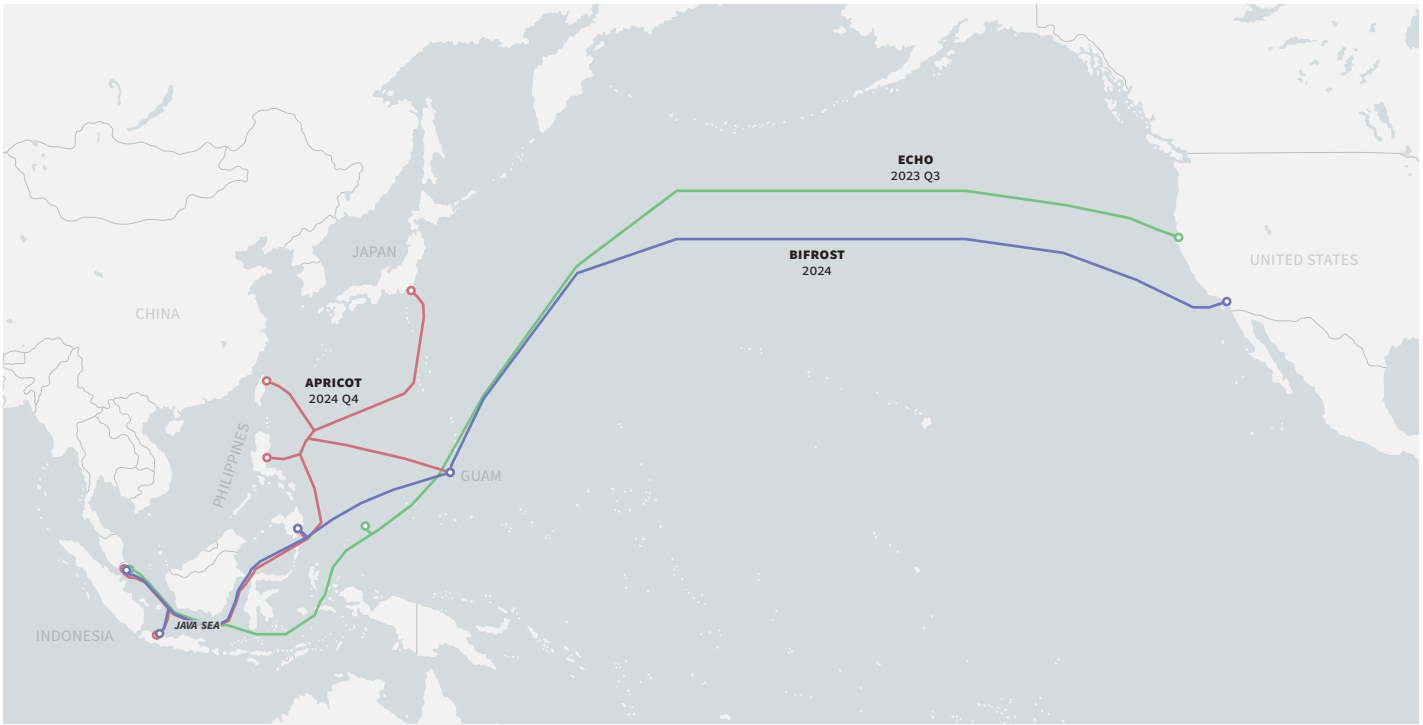
But that advance is attracting scrutiny from regulators, especially in advanced democracies due to predatory pricing. On November 21, 2021, the European Union announced tariffs on several Chinese companies, including Hengtong and Fiberhome Marine, another provider, after an investigation found that they were **dumping** optical fiber cables into the European market at artificially low prices. Fiberhome's parent company was added to the U.S. Department of Commerce's "**Entity List**" in June 2020 for enabling human rights violations and abuses in Xinjiang. Additionally, the Federal Communications Commission has many Chinese telecommunications companies under **revocation** proceedings.

China's ownership of cables has expanded considerably in recent years and is concentrated among China Telecom, China Unicom, and China Mobile. Known as the "Big Three," these state-owned companies control 98.5 percent of China's international bandwidth. The Big Three combined for an ownership stake in 31 cables deployed in 2021. This **trend** is expected to continue, as each company has announced investments in 2022 or 2023.

State support is driving this expansion forward, especially in developing markets. As state-owned enterprises, the Big Three are able to invest in cables with less certain commercial fundamentals. Financing from the Export-Import Bank of China and other state sources allows HMN to offer projects below market rates. As part of a tender process overseen by the World Bank, HMN reportedly submitted a **bid** that was 20 percent below its competitors to build the East Micronesia cable system, encompassing the Federated States of Micronesia, Nauru, and Kiribati.

Not all of these projects have delivered on their commercial promises. In Papua New Guinea, for example, a $298 million loan from the Export-Import Bank of China supported Huawei Marine's construction of the Kumul subsea cable. Inadequate environmental planning left the cable vulnerable to seismic activity, and it was damaged in 2019. Rather than delivering faster internet speeds, the project has contributed to a worrying government **debt load**. Despite this cautionary tale, China's sales pitch—which emphasizes low up-front costs and fast delivery—remains attractive.

Figure 6: Map of New Routes – Apricot, Bifrost, and Echo Cables



Source: TeleGeography, "Submarine Cable Map," https://www.submarinecablemap.com.

SECURITY INNOVATIONS

NEW ROUTES OFFER GREATER RESILIENCY

As they race to provide additional capacity while adapting to the challenges mentioned above, cable builders are planning new routes that increase network resiliency. For example, Echo and Bifrost, two systems expected to be completed by 2024, will be the first transpacific cables crossing the **Java Sea**. Complementing Echo is Apricot, the first intra-Asian subsea cable that does not traverse the crowded part of the South China Sea. These and other transpacific routes that avoid the South China Sea and Hong Kong will be longer and therefore costlier to build and operate. Cable providers are betting that they will build more optionality into networks in the case of outages and avoid the obstacles to operating near Chinese territory.

With these new routes emerging, Indonesia, the Philippines, and Guam are among the countries and territories most likely to increase their centrality in transpacific networks. Indonesia is projected to have a $124 billion **digital economy** by 2025 and has already minted six unicorns—private startups with a valuation of more than $1 billion. Growing the digital economy is integral to President Joko Widodo's plan for Indonesia, the world's fourth most populous country, to become one of the world's five largest economies by 2045.

But maximizing Indonesia's digital potential will require improving regulatory certainty and strengthening cable protection. Indonesia lacks a nationally coordinated policy for subsea cables, and its management of subsea cables is **fragmented** among several government institutions. Cables landing in Indonesia can be vulnerable to anchor dropping, given the presence of crowded international shipping lanes, and extensive fishing.

The Philippines is also poised to rise as a data hub. Several upcoming cables include landing points in the Philippines, including Apricot, and the transpacific systems Bifrost, PLCN, and CAP-1. These landing points can increase route diversity while lowering latency on traffic between Southeast Asia, North Asia, and the United States. Like Indonesia, however, **strict government regulations** in the Philippines can complicate the cable approval and repair process.

Guam has been a strategic waystation for connections between Asia and the U.S. mainland since the first transpacific telegraph cable was completed in **1903**. The island now has one of the most extensive telecommunications infrastructures in the Asia-Pacific region. It provides a point of **interconnection** where subsea cables, which require electricity to power the optical amplifiers of the system, can be recharged. Guam's status as a U.S. territory also offers regulatory consistency for cable planners, reducing the number of national-level approvals for transpacific systems.

Singapore, an incumbent hub in the region, may have less room for growth in the future. The city-state offers a high degree of existing connectivity, but also some of the region's highest prices for data centers. The government of Singapore has also enacted **legislation** halting the construction of new data centers due to their intensive electricity demands and land scarcity. Singapore will still benefit from network effects for years to come, but the risk that it could be a single point of failure and constraints on new development open the door for new hubs to emerge.

BEST PRACTICES INCREASE DATA SECURITY

One conceptual framework for understanding global computer networks is to picture the internet as consisting of three layers. A robust approach to securing data is based on best practices at each of these layers—physical, data, and control—which together can mitigate threats.

Physical Layer

The physical layer of the internet consists of cables, satellites, landing stations, routers, and the power grid. Some of the key physical security issues around subsea cables occur as a cable approaches the shore and is

Figure 7: Best Practices for Cable Security

Source: Authors' own analysis.

connected to a cable landing station (CLS), the point where data is converted to a terrestrial cable. The site must be chosen carefully, as marine traffic and sediment movement can damage or uncover buried cables. With climate change exacerbating extreme weather events, there is an increasing trend toward hardening these sites, such as by raising the first floor of a CLS to protect against flooding.[4]

Within CLS locations, a detailed set of requirements designed to protect against malicious activity are built into contracts between cable providers and managers of data center colocation facilities. Every entrance and exit to the facility is monitored using a security system with access cards and badge readers, while entrances are configured as mantraps, interlocking doors that can trap unauthorized entrants. Example operational standards include staffing 24/7 with in-house security personnel and requiring escorted access in highly restricted areas.

In addition to these measures, the "fit-out" approach requires each cable owner using a colocation facility to maintain separate locked cages for their equipment. Separability ensures that there are no shared vulnerabilities, as cable builders can select their own third-party vendors for submarine terminal line equipment and add additional security measures to the cage itself, such as different access control approval lists and welded wire mesh cage walls.

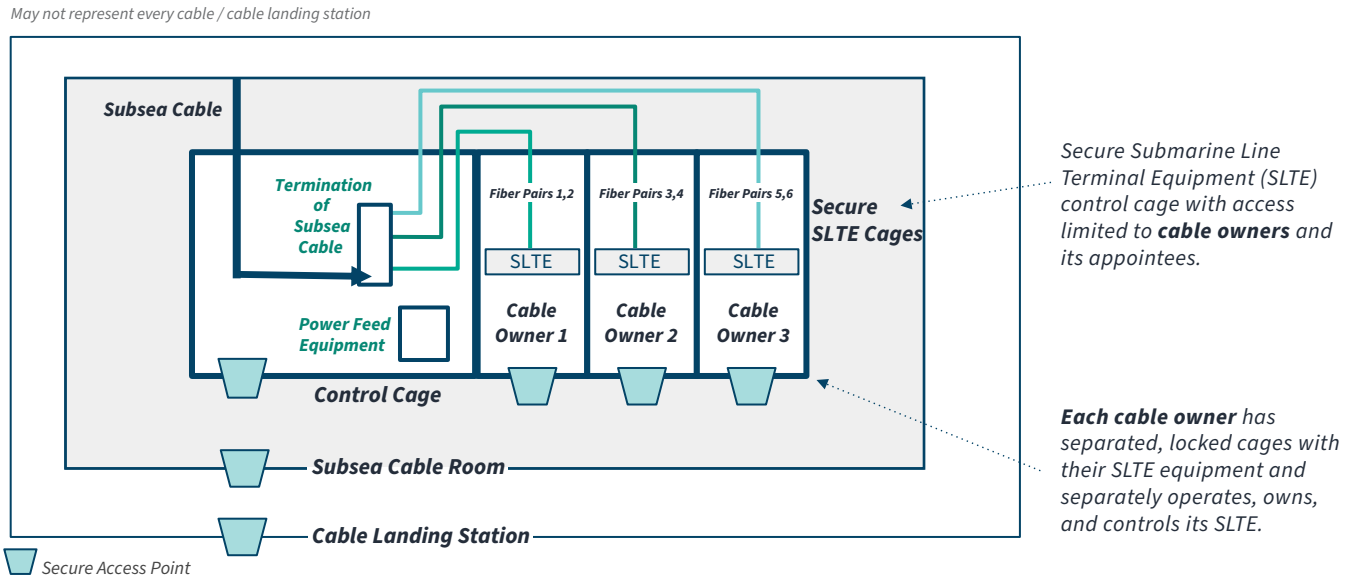
Data Layer

The data layer consists of anything involving actual traffic flow and content. The primary defense used on the data layer for subsea cables is encryption, which is designed to ensure confidentiality in spite of any lapses in physical or operational security practices. **Conventional encryption** methods work by using an algorithm and a public key to transform an input into an encrypted output. The receiving party uses the corresponding private key—a mathematically associated companion to that public key—in order to decrypt the transmission. However, to any unauthorized recipients, the message will appear as unreadable text.

Encryption standards are developed through a rigorous peer review process driven by government and academic experts. Content providers do not develop their own encryption but rely on standards-setting bodies such as the National Institute of Standards and Technology (NIST) and the Internet Engineering Task Force, which have spurred development of protocols such as transport layer security (TLS). Session-based encryption keys make it even more difficult for bad actors to access data in transit. Particular session keys for TLS generally last for a short period of time and a particular data stream may include millions of individual keys per second.

While it has been theorized that quantum computing may make it easier to decrypt traffic using certain kinds of cryptography, the technology is at least a decade away from becoming viable. In the meantime, various government institutes, including NIST, are actively working to develop countermeasures. For example, quantum key distribution

Figure 8: Landing Station Security Measures



Source: Google LLC.

(QKD) works by encoding each bit of the cryptography key on a single photon. If an eavesdropper attempts to read or intercept the transmission, the information encoded on the photon will be lost and the interception will be observable, alerting the communicating parties to the interference. QKD has been **proven to work** over existing submarine optical telecommunications fiber. Cable builders have also experimented with another road to quantum-safe networks, **post-quantum cryptography**, which uses a hybrid key exchange to shield data in transit.

Control Layer

The control layer governs how data is routed around the global public internet. Collections of routers use **Border Gateway Protocol** (BGP) to exchange information, enabling them to calculate the most efficient routes to send packets. However, as a vestige from the early days of the internet, BGP assumes all networks are trustworthy, creating an exploitable vulnerability.

By collaborating and sharing threats, network operators can further protect the control layer. Mutually Accepted Norms for Routing Security (MANRS), a community-driven initiative launched in 2014, provides fixes for the most common routing threats. By signing on to MANRS, network operators agree to practice actions such as maintaining accessible contact information and enabling source address validation, ensuring that BGP operates in a more secure manner.

Because subsea remote management systems are operated as a separate network on a private backbone, they are not generally susceptible to these general routing issues. Active and passive external network scanning for policy validation provides another layer of protection.

Zero-Trust

Another tactic for securing data throughout the layered internet is practicing "zero-trust" principles. The **zero-trust approach** *assumes* cybersecurity breaches within organizations and verifies each request as though it originates from an open network. These principles apply to identity, end points, applications, data, infrastructure, and networks. Segmenting networks into smaller silos can limit the blast radius of a cybersecurity incident and ward against internal bad actors.

The zero-trust approach enhances data security in the complex environments in which subsea cables are built. These include operations in foreign territory, partnerships with co-owners, or the use of equipment provided by third-party suppliers.

NETWORK FUTURES

This section will examine three possible futures that hinge on the actions taken by U.S. policymakers. The first two of these scenarios would likely be detrimental to U.S. interests. If the current defensive policy trajectory is intensified, Chinese and American spheres of internet influence will further separate and bring on unintended consequences. A second future looms in which China continues to expand its role in cable projects and supplants the United States as the region's central hub. U.S. policymakers can avoid these outcomes by acting assertively to support the building of secure cable systems while galvanizing regional partnerships.

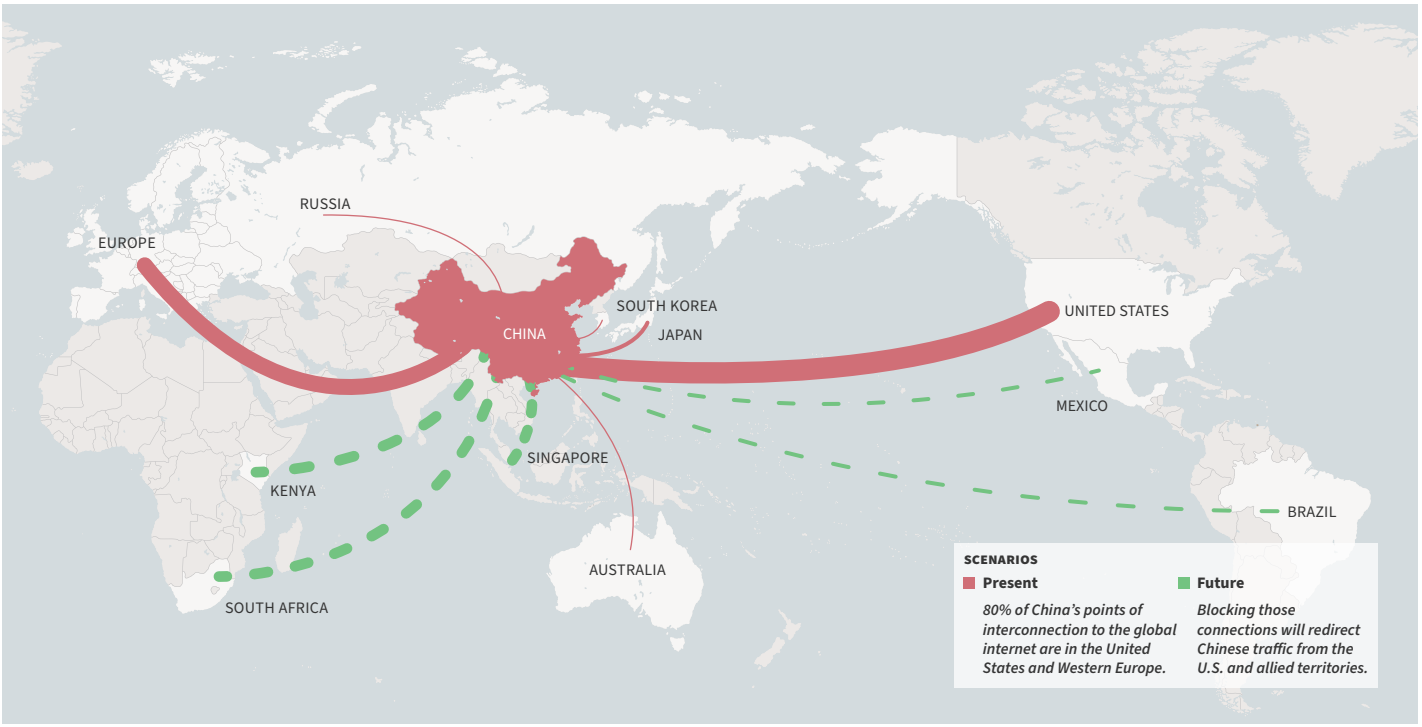
PLAYING DEFENSE

In the first scenario, U.S. policymakers adopt a well-intentioned but overly defensive posture that ends up harming both strategic and commercial interests. To date, policies have included **revoking** the licenses of China Telecom and its U.S. subsidiaries to provide telecommunications services in the United States as well as **canceling** or **revising** four cable projects with links to Hong Kong. Future measures could involve reducing Chinese points of presence in the United States, nodes where two or more networks share a connection. A further escalation would be banning cable connections between the United States and untrusted countries and banning U.S participation in cable ownership consortia with untrusted entities. These actions could also cause China to exert similar restrictions on U.S. companies, reducing their ability to build infrastructure in the rapidly growing Asia-Pacific region.

While superficially appealing, these actions would be based on misconceptions about internet infrastructure. The world's largest internet hubs are neutral and open; therefore, many non-domestic telecoms have multiple points of presence in the United States. China is an outlier in that it prohibits foreign telecom operations within its borders, meaning its **connections** to the global public internet occur mainly in Western Europe and the United States. Balkanizing the internet will erode the United States' strategic advantage, as the points of direct physical interconnection will be relocated from U.S. and allied soil to areas with less technical oversight, as illustrated in Figure 9. Third-party countries hosting connections may also lack security standards or be heavily indebted to China.

In this future, alternative routes that do not reflect U.S. interests are more likely to emerge. Projects such as a

Figure 9: Scenario 1 – Playing Defense



Source: Dave Allen, "Analysis by Oracle Internet Intelligence Highlights China's Unique Approach to Connecting to the Global Internet," Oracle, July 19, 2019, https://web.archive.org/web/20210512021539/https://blogs.oracle.com/internetintelligence/analysis-by-oracle-internet-intelligence-highlights-china%E2%80%99s-unique-approach-to-connecting-to-the-global-internet.

recent Canada-Japan cable will become more common, and Asia-Mexico cable systems will be seriously considered. In addition, if companies avoid landing cables in the United States, many U.S. services may experience additional latency, possibly limiting the potential of real-time applications, increasing the costs of data transport for U.S. data, and decreasing the market share for U.S. subsea cable companies. With existing routes revised, it would become *more* difficult to detect whether China is intentionally misdirecting data flows, such as a suspicious **2019 incident** during which traffic for some of Europe's largest mobile networks was routed through China Telecom for a little more than two hours.

CEDING THE FIELD

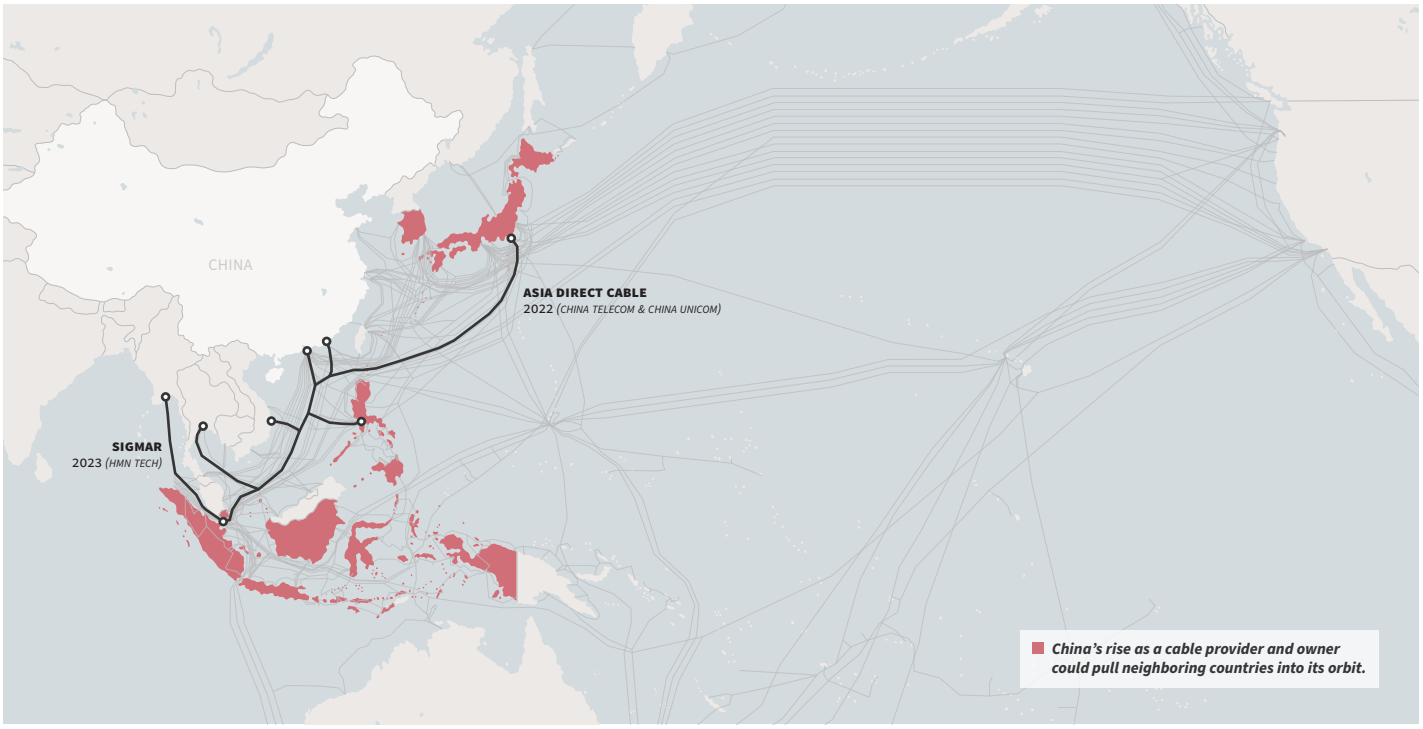
A second scenario, which could play out simultaneously to the first, is one in which China rapidly reshapes Asia's network topology in its favor. Just as China is moving ahead with arrangements that create favorable patterns of trade, it is eager to create favorable patterns of data flows. If the United States is too slow to respond to such actions, it will miss the opportunity to meet growing bandwidth demand and to signal enhanced U.S. economic engagement in the region.

Sluggishness could stem from a lack of policy clarity, predictability, and speed. Each cable that lands in the United States must receive approvals at the federal, state, and local levels. They must also pass an interagency national security review (formerly known as Team Telecom), which evaluates the national security and law enforcement implications of foreign investment in U.S. telecommunications networks and makes a recommendation to the Federal Communications Commission. This exhaustive review averaged **eight and a half months** for applications submitted between 2017 and 2019.[5] **Singapore's** process takes only three months and is highly predictable.

In this scenario, China entices developing countries with below-market offers, cribbing from the same playbook it has used across a range of infrastructure investments to expand its digital footprint. Emerging hubs such as the Philippines and Indonesia would become less attractive for U.S. connections, and Asian internet service providers would form a more tightly knit series of physical connections with China, as shown in Figure 10. This would make it increasingly likely that more countries would adopt China's data governance policies.

HMN would capture a greater market share of the cable industry, while the "Big Three" would expand their access

Figure 10: Scenario 2 – Ceding the Field



Source: TeleGeography, "Submarine Cable Map," https://www.submarinecablemap.com.

to foreign data. China would benefit commercially and strategically, as the region would become more vulnerable to economic coercion, with more internet chokepoints under government control. China has **weaponized** other transnational flows in the past, cutting off trade, tourism, and investment with partners as leverage in political disputes.

GOING ON OFFENSE

In the third, optimal scenario, the United States redoubles its emphasis on offensive, market-opening measures in coordination with allies, illustrated in Figure 11. Financial assistance for developing countries would provide an incentive to link to U.S.-centered networks and help close the global digital divide. Pacific Island nations have a discrete need for more affordable and reliable internet delivery, while emerging economies are eager to build out their international capacity. Expanded prosperity throughout the region would not only accrue goodwill but benefit U.S. workers and companies.

Fortunately, there are a number of key partners willing to help accomplish these goals. Wary of China's growing influence, Japan and Australia have been proactive about ensuring subsea cable security and providing viable alternatives to Chinese bids. **Japan** recently announced a $440 million outlay toward subsea cable and data center decentralization, while Australian aid paid for the Coral Sea Cable system linking to Papua New Guinea and the Solomon Islands, muscling out hardware from **Huawei Marine**.

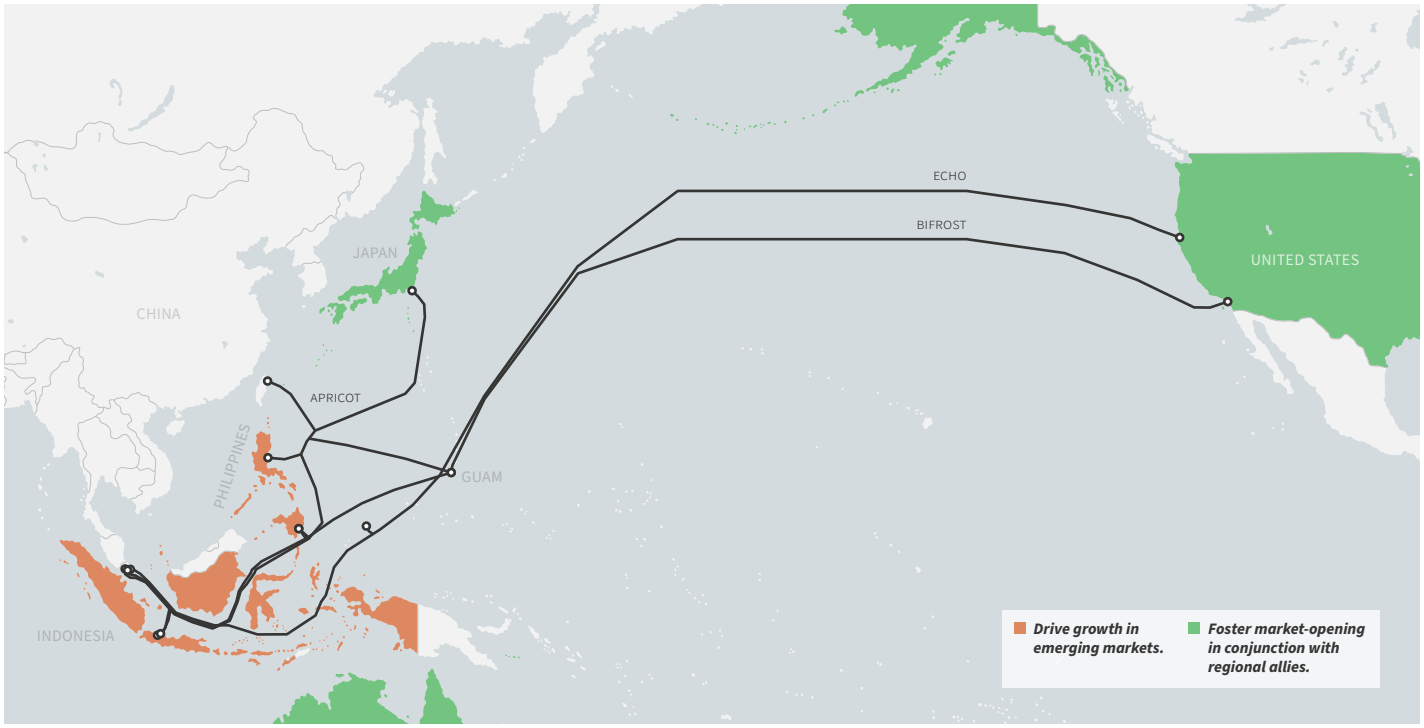
By going on offense, the United States can build out a global digital infrastructure coordination group that considers and evaluates a rapidly changing landscape to enable further private sector investment. There is regional precedent for this kind of collaboration. The Trilateral Infrastructure Partnership between Japan, Australia, and the United States jointly funded a subsea cable extension in **Palau** and has committed to financing the **East Micronesia** cable system.

RECOMMENDATIONS

To realize a future in which the United States maintains its status as the world's leading internet hub, policymakers need to devote sustained attention to Asia's growing bandwidth demands and changing cable networks. The following policy actions would advance U.S. economic and strategic interests.

1. Pursue subsea cable objectives in regional digital agreements. There is a clear need for more comprehensive and consistent global rules governing subsea cables. An important start would be for the United States to ratify the **United Nations Convention on the Law of the Sea**, which provides subsea cables international legal protections.

Figure 11: Scenario 3 – Playing Offense



Source: TeleGeography, "Submarine Cable Map," https://www.submarinecablemap.com.

Several regional platforms provide an opportunity to further develop **U.S.-preferred digital norms** and values in the Asia-Pacific region. The United States should join the **Digital Economy Partnership Agreement**, signed by Singapore, New Zealand, and Chile in 2020, and negotiate a new module of work that sets standards for subsea cable initiatives. Singapore has already built articles governing subsea cables into its bilateral Digital Economy Agreements with **Australia** and the **United Kingdom**. Standards would include criteria for screening and certifying cable vendors to ensure secure data flows. To expand the regional impact, this could serve as a template for a similar line of work in the proposed **Indo-Pacific economic framework**.

2. Promote cable best practices in key countries. The United States should engage diplomatically with key countries in the region, such as Indonesia and the Philippines, to promote good regulatory practices for safe and efficient cable operations. Encouraging these countries to adopt **the International Cable Protection Committee's (ICPC) best practices** would be another promising step in this direction. The ICPC urges states to act on statistically significant threats to cables where government policies could mitigate risk, such as designating anchorages and enforcing recommended separation distances between cable ships and other vessels. One particular area of focus should be exempting subsea cables from cabotage laws, which prevent foreign vessels from performing cable repairs; this issue led to Malaysia being excluded from the Apricot cable. Another emphasis should be advocating for national policies on deep sea mining that are consistent with efficient cable operations.

3. Coordinate within the U.S. government and with regional allies and partners. There is no shortage of private capital for subsea investments, but better coordination is needed to compete with China. Building on the strength of their premier firms, the United States and its allies need to be able to provide reliable, timely, and efficient subsea cable systems. Internally, the U.S. government needs to establish a centralized team—drawn from relevant agencies such as the State Department, the Department of Commerce, the U.S. Agency for International Development, and the Development Finance Corporation—that can elevate digital infrastructure as a policy priority. U.S. engagement in subsea cable issues should be aligned externally with regional allies and partners such as Japan and Australia. These efforts can complement initiatives such as the G7's **Build Back Better World** and the U.S.-EU Trade and Technology Council's **Information and Communication Technology and Services working group**, while financing for edge cases such as the Palau spur can be provided by the International Finance Corporation and

other multilateral development banks. This will ensure that U.S. agencies are amplifying support for efficient and trusted cable systems built by the private sector while fostering allied cooperation.

4. Expand and adopt zero-trust technologies. Rather than prohibit the operation of cables in untrusted environments, the United States should strive for security protocols that ensure data security while maintaining the openness and neutrality of the global internet. Advanced intrusion sensors can monitor seabed cables, while physical landings can be fortified by encouraging and incentivizing best design and operational practices. In particular, the United States should increase public funding for quantum communications technology and work in partnership with industry stakeholders and allies to develop possible applications for protecting sensitive data in transit.

5. Increase transparency and predictability of licensing and permitting. The U.S. security review process for cable projects is opaque and can create undue uncertainty and delay. While it is important that technologies critical to national security are thoroughly vetted, the interagency committee evaluating international undersea cables should establish and disseminate clear guidelines with cable builders to communicate the specifications for review requirements and timeframes. Each delay or restriction comes with a significant financial impact and places U.S. companies at a competitive disadvantage. These changes would resolve uncertainty around the status of existing connections and cut down on review timelines for new applications. Another benefit of greater regulatory clarity is more opportunities for public-private partnerships that boost the connectivity of developing economies. It is not cost-prohibitive to build a branching unit into a larger privately financed cable during the design phase but doing so requires effective coordination. ■

Matthew P. Goodman *is senior vice president for economics at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Matthew Wayland*** *is a research assistant with the CSIS Reconnecting Asia Project.*

The authors wish to thank the many experts and officials who attended the three roundtables associated with this project and provided helpful comments on drafts of this brief. The analysis and views in this brief are solely those of the authors.

This brief is made possible by generous support from Amazon, Google, Meta, and Microsoft.

ENDNOTES

1 Subsea cables serve several U.S. strategic interests as well, such as promoting development, supporting democratic access to information, and facilitating government communications. For more, see: https://www.csis.org/analysis/securing-subsea-network-primer-policymakers.

2 A recent **study** of Malaysia estimated that subsea cables added 6.9 percent to its GDP. Another **study** projects that connecting Indonesia to the Apricot, Bifrost, and Echo cables will have a GDP impact of $59 billion between 2023 and 2025.

3 These eight **cable systems** are Jupiter, TOPAZ, H2 Cable, Southern Cross NEXT, SxS, Echo, Bifrost, and HCS.

4 When Hurricane Sandy pounded the East Coast of the United States in October 2012, the **entire network** between North America and Europe was isolated for a number of hours due to the concentration of cables in New York and New Jersey.

5 However, under an April 2020 executive order (**13913**), which established the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, the **reviews** may not last more than 210 days.