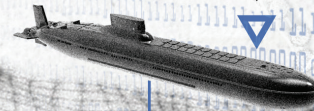


THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

June 27, 2023



The Escalating Global Risk Environment for Submarine Cables

Executive Summary

Submarine cables, the information superhighways that underpin the global economy and facilitate worldwide telecommunications, are operating in an increasingly complex and dynamic risk environment. The rapid expansion and evolution of the submarine cable network — fueled by the voracious data demands of mobile users, cloud-based computing, and the business imperatives of hyperscalers such as Amazon, Google, Meta, and Microsoft — must contend with converging geopolitical, physical, and cyber threats.

State actors are almost certainly the greatest threat with regard to intentional sabotage and spying, given their capabilities and strategic incentives. Non-state actors, including hacktivists and ransomware groups, pose a less capable and lower likelihood threat to the networks and operating systems that submarine cables rely upon, but their threat cannot be discounted. Accidental damage from ship anchors or fishing vessels are higher frequency, but lower impact events.

Major geopolitical developments, specifically Russia's war against Ukraine, China's increasing coercive actions toward, and preparations for, a potential forceful unification with Taiwan, as well as the deepening rift between Beijing and Washington, will very likely be key drivers of the near-term risk environment. The growing role of Chinese state-owned enterprises as cable owners and providers has introduced rising concerns of digital surveillance amid a reshaped internet architecture. Russia, eager to inflict pain on the West for its support of Ukraine, has demonstrated an increased intent to map the submarine cable system, very likely for potential sabotage or disruption. Furthermore, the relentless push for expanded bandwidth capacity has led cable system operators to embrace advanced network management systems, potentially enabling cyberattacks that exploit third-party vulnerabilities.

Key Findings

- Increasing reliance on internet-based connectivity for global finance, telecommunications, government decision-making, and military operations make submarine cables attractive targets for intelligence collection or sabotage.
- The expanding role of Chinese companies in deploying, owning, and operating submarine cables increases the risk of espionage for the countries and companies that use them.
- Hyperscalers such as Amazon, Google, Meta, and Microsoft have shifted from being capacity buyers to direct submarine cable owners, creating new incentives for cable deployments, and introducing new concerns over market monopolies and digital sovereignty, particularly in historically underserved regions.
- Russia's ongoing war against Ukraine, China's preparations for potentially forcefully unifying with Taiwan, and the deterioration of US-China bilateral relations will very likely fuel physical attacks and intelligence collection efforts directed against the submarine cable system to undermine the economic, diplomatic, and national security objectives of the US and its western allies.
- Submarine cable owners and operators will likely continue to turn to third-party providers for remote network management systems to maximize efficiencies and cut costs, very likely creating an avenue for threat actors to target submarine cable infrastructure and data by exploiting cybersecurity vulnerabilities.

Background

Submarine cables have been used for international communication for over 170 years, beginning with a cable [laid](#) across the English Channel in 1850 to carry telegraph messages between England and France. Today, an estimated 99% of intercontinental internet traffic and data and voice communication is [transmitted](#) along fiber-optic submarine cables laid along the ocean floor. These cables are the backbone of the global economy, [facilitating](#) more than \$10 trillion of financial transactions daily, while [conveying](#) sensitive government communications and supporting overseas military operations. In short, they are critical infrastructure for national security purposes, indispensable to a fully functioning modern society.

Faster, cheaper, and more reliable than satellite-based telecommunications, submarine cables are [poised](#) to become even more important as the number of internet users and their devices [continues](#) to [grow](#) rapidly, driving a precipitous rise in the volume of data transiting global networks. According to one industry estimate, global mobile data traffic is [expected](#) to increase at a compound annual growth rate of nearly 28% between 2022 to 2030, reaching 603.5 million terabytes per month. To meet this huge growth in data traffic, cable system owners and providers are quickly expanding capacity. Currently, there [are](#) an estimated 529 cable systems in operation around the world, more than [double](#) the number from 2013, and the rate in new deployments is accelerating, as shown in **Figure 1**.

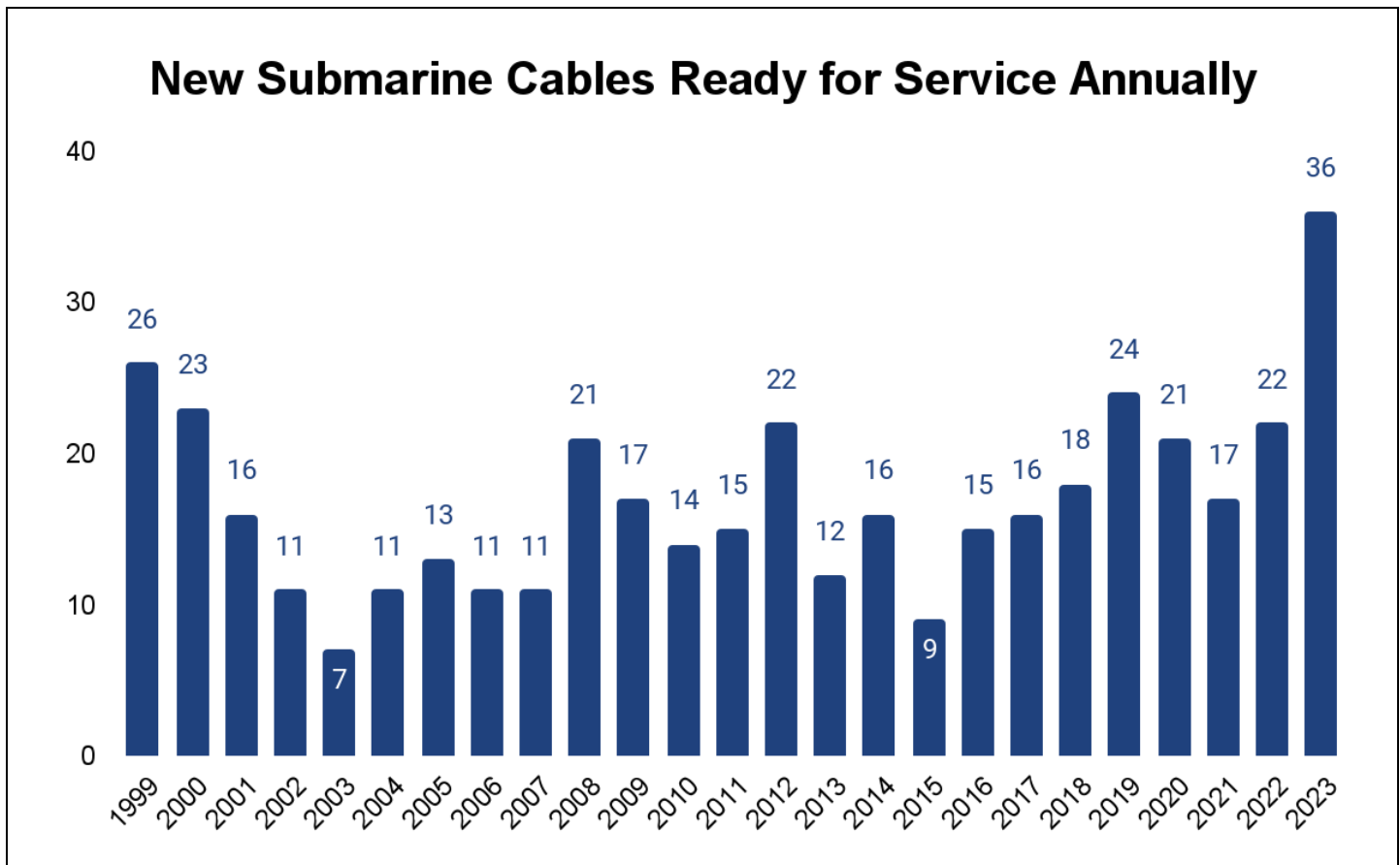


Figure 1: Number of new submarine cable systems ready for service annually between 1999 to 2023 (Source: Recorded Future visualization of [TeleGeography](#) data)

A Primer on Submarine Cables

Submarine cables consist of delicate fiber-optic strands of glass, which [transmit](#) data as pulsed light signals, [wrapped](#) in layers of plastic, steel wires, copper sheathing, and polyethylene insulation. Approximately the diameter of a garden hose where they lay across the deepest parts of the ocean, the cables are encased in thicker armor to defend against errant ship anchors as they approach the shoreline. Submarine cables can contain a range of fiber pairs, now [reaching](#) as many as 24, whose bandwidth can be owned or used by multiple parties. The bandwidth capacity of these cables is similarly expanding at a rapid rate: the transatlantic Apollo cable, ready for service in 2003, was initially capable of [transmitting](#) under 1 terabit per second (Tbps) per fiber pair, but subsequent design enhancements in 2015 boosted its capacity to 8 Tbps. Newly designed cables are capable of significantly greater throughput, as demonstrated by Google's transatlantic Dunant cable, [deployed](#) in 2023, which has a design capacity of 25 Tbps per fiber pair. However, cables typically only use roughly 20% of the total design capacity (the "lit" portion) to provide a buffer against surging demand or rerouted traffic.

A submarine cable system is [divided](#) into 2 parts: the “wet” plant, made of the cable itself and repeaters or amplifiers placed along the cable to boost the signal, and the “dry” plant, where the cable arrives onshore, is routed through a beach manhole, and arrives at the landing station to be connected with terrestrial networks (**Figure 2**). Network management tools and power feed equipment are provided at each landing station, dictated by the length and complexity of the cable architecture. Tata’s 13,000 kilometer TGN-Atlantic, for example, [receives](#) approximately 9,000 volts.

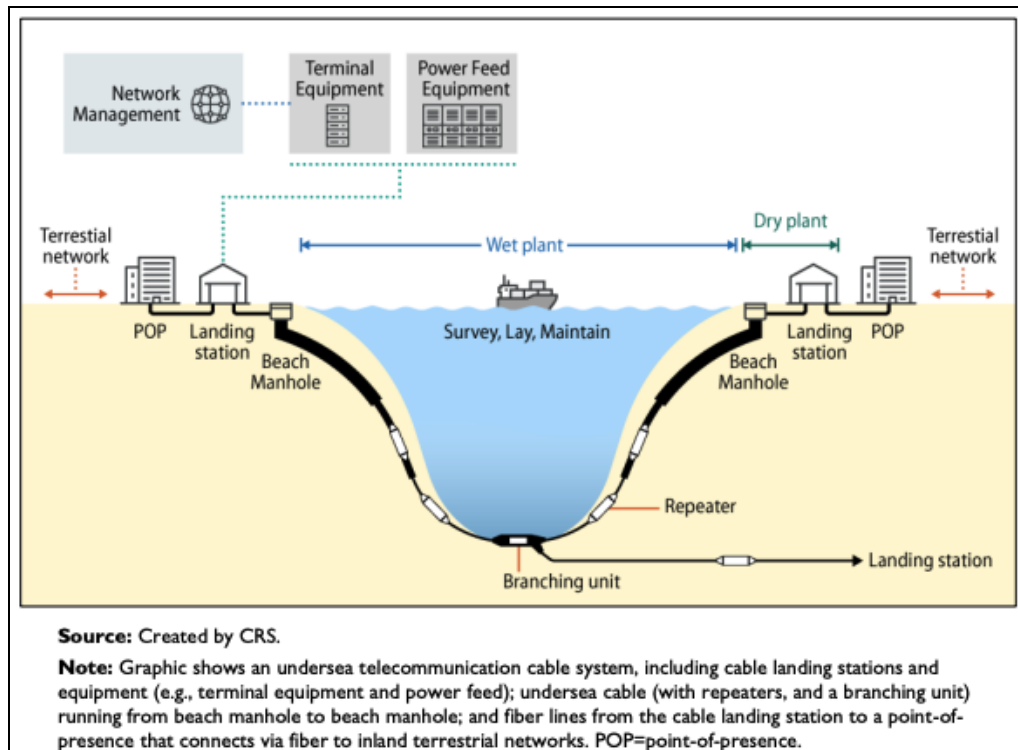


Figure 2: Submarine cable system (Source: [Congressional Research Service](#))

The Escalating Global Risk Environment

The rapid expansion and evolution of the global submarine cable network in the twenty-first century has brought new risks into sharper focus, reflecting the convergence of geopolitical, physical, and cyber threats. A changing ownership landscape, featuring the rising involvement of Chinese state-owned enterprises and a growing role for hyperscalers,¹ has introduced new geopolitical considerations and altered the physical topography of the internet. The proliferation of cables and their attendant landing stations has created new opportunities for threat actors to engage in physical security attacks or conduct espionage. And the embrace of remote network management systems to enhance system capacity could facilitate cyberattacks on cable system infrastructure and exploitation of the data it carries.

¹ Hyperscalers are typically [defined](#) by their ability to rapidly and efficiently scale infrastructure in response to demand, with particular emphasis on cloud platforms and data centers.

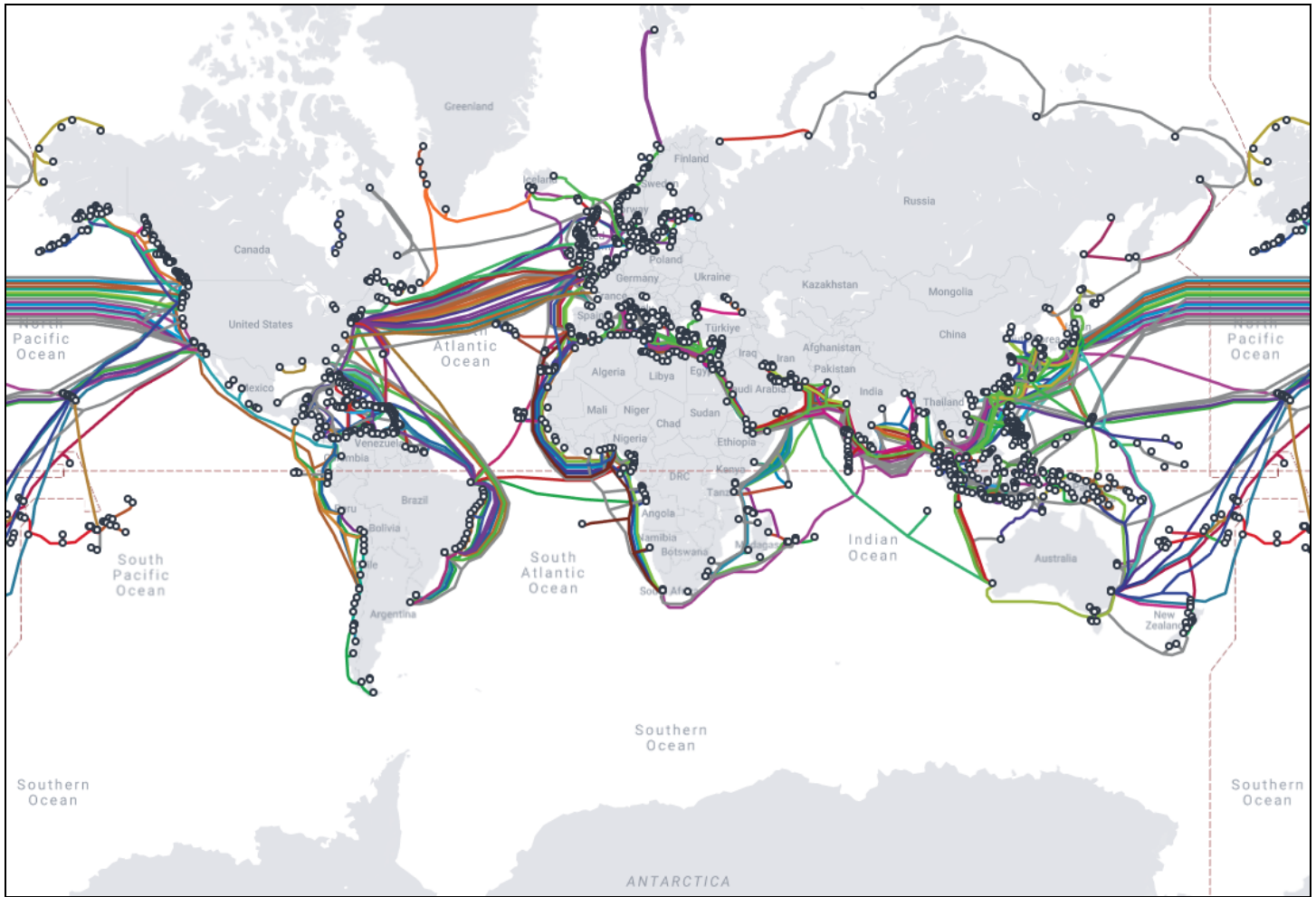


Figure 3: Map of submarine cables as of May 16, 2023 (Source: TeleGeography's [Submarine Cable Map](#))

An Evolving Production and Ownership Landscape

Growing Chinese Stake

Over the last decade, Chinese state-owned or -affiliated enterprises have sought a greater stake in the global submarine cable network, almost certainly increasing China's ability to manipulate, [surveil](#), and [interfere](#) with worldwide data flows. The production and ownership of a submarine cable system is typically divided between 2 groups of entities. Traditionally, the three largest [providers](#) of cable manufacturing and deployment globally have been US-based Subcom, France-based Alcatel Submarine Networks, and Japan-based NEC Corporation. Ownership of submarine cables, however, is more highly fragmented, with companies sometimes choosing to co-own a cable to build an expansive market presence geographically, offset costs, and divide operational and maintenance responsibilities. In both categories, China has rapidly advanced. Hengtong Optic-Electric (owner of HMN Technologies, formerly known as Huawei Marine Systems), now owns 10% of the cable laying market, and 3 state-owned Chinese telecom providers — China Mobile, China Telecom, and China Unicom — have [ownership stakes](#) in nearly 40 cables.

China has historically focused on laying cables around mainland China, Hong Kong, and Taiwan; in recent years, however, Chinese companies have [increased](#) their [involvement](#) in [deploying](#) cables globally, especially in Southeast Asia, the Middle East, and Africa, as [part](#) of the technology element of China's Belt and Road Initiative (BRI), often referred to as the Digital Silk Road. Huawei Marine Systems, originally [created](#) as a joint venture of Chinese telecom giant Huawei and UK-based Global Marine Systems, has led this expansion due to its ability to provide significantly cheaper installation pricing, [prompting](#) speculation it was subsidized by the Chinese government — a claim the company has repeatedly denied.²

Concerns over Huawei's [allegiance](#) to Beijing were not alleviated by the company's sale to Shanghai-based Hengtong Optic-Electric in 2019 and Huawei Marine Systems' subsequent [rebranding](#) as HMN Technologies in 2020. Hengtong has previously worked with the Chinese government on BRI projects, indicating it is a trusted partner.³ Moreover, the company's founder and head of its board of directors, Cui Genliang, is [reportedly](#) a former telecommunications specialist for the People's Liberation Army. As a result of these linkages, the US and other western countries have sought to cancel or forestall projects involving Huawei Marine/HMN Technologies. In 2018, the Australian government [ousted](#) Huawei from a cable project connecting Australia with Pacific Island nations due to [concerns](#) by the Australian Security Intelligence Organization (ASIO) over espionage. In 2020, the US [warned](#) Pacific Island nations about Huawei Marine's involvement in a cable linking the Federated States of Micronesia (FSM), Kiribati, and Nauru, leading to the decision to [award](#) the contract to an Australian provider. Finally, in December 2021, the US Department of Commerce [imposed](#) Entity List sanctions against HMN Technologies.

The ongoing expansion of the global submarine cable network, however, has provided HMN Technologies with continued business opportunities. According to a 2020 Federal Communications Commission (FCC) report, while still operating under the Huawei Marine name, the company had [built](#) or repaired almost 25% of the world's cables. Over the next 2 years, HMN Technologies is currently [slated](#) to supply cable for 3 projects underway in Asia (**Figure 4**). It will also serve as the provider for a recently [announced](#) \$500 million China-led cable network connecting Hong Kong, Hainan Island, Singapore, Pakistan, Saudi Arabia, Egypt, and France. This sprawling project is [envisioned](#) as a direct competitor to the US-led [SEA-ME-WE 6](#) cable network, which HMN Technologies was removed from at the behest of the US.

² [https://www\[.\]huawei\[.\]com/en/facts/voices-of-huawei/no-huawei-isnt-built-on-chinese-state-funding](https://www[.]huawei[.]com/en/facts/voices-of-huawei/no-huawei-isnt-built-on-chinese-state-funding)

³ [https://eng\[.\]yidaiyilu\[.\]gov\[.\]cn/](https://eng[.]yidaiyilu[.]gov[.]cn/)

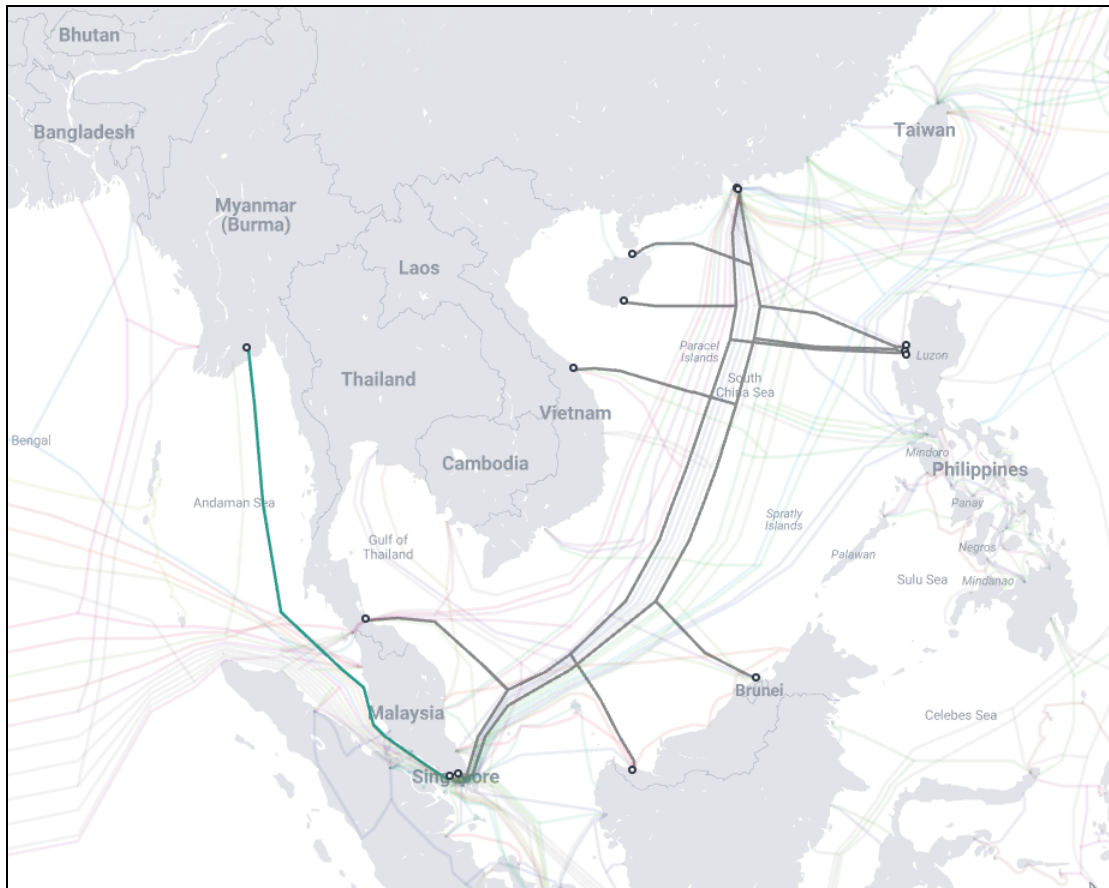


Figure 4: Currently planned HMN Technologies cable deployments, 2023-2025
(Source: TeleGeography's [Submarine Cable Map](#))

In parallel with its push into the cable production and deployment sector, China has sought to expand its stake as an owner/operator of cables across the world. This shift provides China with a greater ability to dictate where and how submarine cables are deployed, very likely supporting its geopolitical ambitions while creating new opportunities for intelligence collection through the landing stations it controls. This expansion has also given Beijing greater ability to [shape](#) the physical structure of the internet, and potentially its corresponding digital behavior. By one analyst's [count](#), prior to 2021, China's state-owned telecom providers owned 3 submarine cables (2 belonging to China Telecom, 1 to China Mobile). That number [increased](#) to 34 cables between 2021 and 2022, distributed among China Telecom, China Mobile, and China Unicom.

Reflecting these dual concerns over China's ability to control digital flows, the US has actively exercised its regulatory powers to prohibit Chinese participation in ownership groups involving cables connecting to the US. In June 2020, the US interagency body informally known as "Team Telecom" [recommended](#) the FCC deny an application by Meta and Google to connect Los Angeles, California, to Hong Kong via the Pacific Light Cable Network (PLCN). Among its concerns, the US Department of Justice (DOJ) cited China's "sustained efforts to acquire personal data of millions of U.S. persons" and the possibility that the PLCN would advance China's goal of establishing Hong Kong as a key hub for digital traffic.

Ultimately, the PLCN [moved](#) forward without Chinese ownership or landing stations. Although China will almost certainly continue to be stymied in its efforts to establish direct connectivity with the US mainland, it will very likely find success in building networks across Asia/Pacific and traditionally underserved markets, most notably Africa:

- A subsidiary of Hengtong Group, with the assistance of HMN Technologies, recently [completed](#) the Pakistan & East Africa Connecting Europe (PEACE) submarine cable, bridging Singapore, Pakistan, Kenya, Egypt, and France, among other countries.
- China Telecom recently [completed](#) the Hong Kong landing of the [Asia Direct Cable](#), which will link mainland China, Japan, the Philippines, Singapore, Thailand, and Vietnam.
- China Mobile is [part](#) of a global ownership consortium of the [2Africa cable project](#), which will connect 46 cable landing stations in 33 countries across Africa, Asia, and Europe when it is completed in 2023/2024.
- China Mobile will partially own the Southeast Asia-Japan Cable 2, which will [connect](#) mainland China, Japan, South Korea, Singapore, Taiwan, Thailand, and Vietnam when it is deployed in 2024.
- China Telecom will partially own the Asia Link Cable, which will [connect](#) mainland China, Brunei, Cambodia, the Philippines, Singapore, and Vietnam when it is deployed in 2025.

Rise of the Hyperscalers

As China has taken a more prominent role as an owner/operator in the submarine cable industry, new key players have also emerged in the private sector. Previously, major telecommunication providers like [AT&T](#) were key stakeholders in the cable ecosystem, selling bandwidth to private companies. Beginning in 2010 with Google's [investment](#) as a part-owner of the Unity-EAC Pacific cable system, and [accelerating](#) around 2015, hyperscalers — which also include Amazon, Meta, and Microsoft — began taking a more leading role in the development of the global cable network, [dictating](#) where cables go and the countries they connect.

Unlike traditional telecommunication providers intent on connecting users at endpoints typically co-located with major population centers, hyperscalers seek to connect data centers to data centers, which are often placed in more economical, and less populous, locations. Google's recently [completed](#) Equiano and Firmina cables, which connect locations in South America and Africa, illustrate this approach. From there, these cables are used to supply terrestrial data networks, bringing internet connectivity to these regions.

Meta and Google have each moved rapidly to build submarine cable systems they own outright or in partnership with other entities, currently [owning](#) 16 and 21, respectively. Microsoft and Amazon collectively have ownership stakes in 6 more. Although this ownership stake appears relatively small, totaling approximately 8% of the 529 current cable systems in operation, the trend is accelerating. Of the 102 total submarine cable systems deployed between 2018 and 2022, hyperscalers have an ownership role in roughly 22.5% of them (**Figure 5**). The economics driving this decision-making are

simple: taking a direct ownership role becomes more cost-effective as data use skyrockets. Between 2012 and 2022, hyperscalers' share of total cable data capacity [climbed](#) from approximately 10% to 71%. It also enables the hyperscalers to establish cable connections at a time and location that best fits their business requirements.

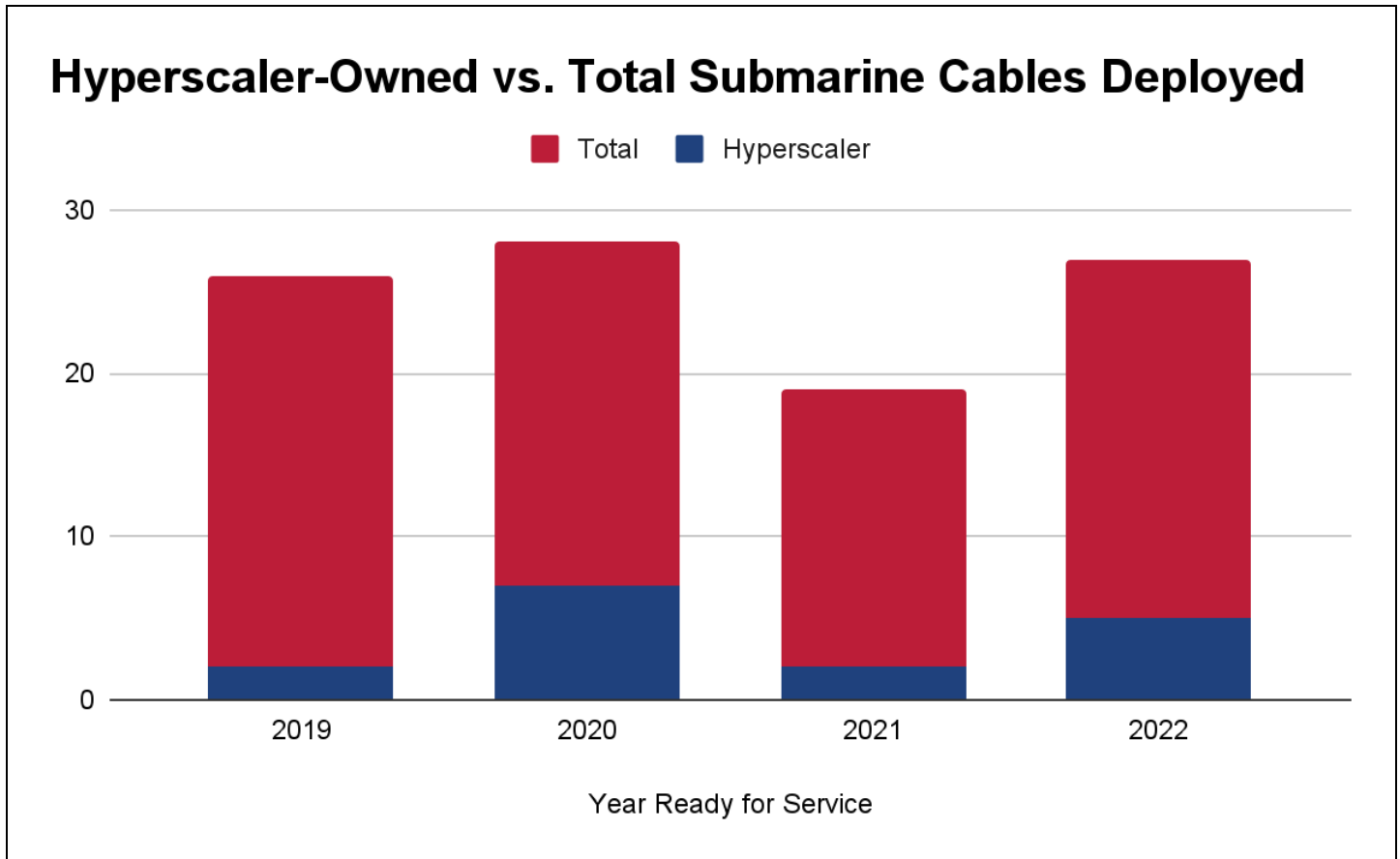


Figure 5: Hyperscaler-owned cable systems ready for service, 2018 to 2022
(Source: Recorded Future visualization of [TeleGeography](#) data)

Historically, cable ownership structure has been heavily [weighted](#) toward single entities versus multiple entities: roughly two-thirds of all cable systems are owned by a single company. Recent data indicates this trend remains unchanged. In 2022, 82% of the 22 cables deployed were solely owned, and of the 36 cables scheduled to be ready for service in 2023, 66% are solely owned.⁴

Each ownership structure presents unique complexities and limitations. Single owner systems often provide smaller geographic coverage, encompassing shorter cable runs or runs with a limited number of landing points, such as the [Natitua Sud](#) in French Polynesia or the [Unitel North Submarine Cable](#) connecting parts of Angola. Multiple owner systems, which are managed as multinational consortiums, are capable of financing and operating significantly more complicated cable systems, such as the previously mentioned SEA-ME-WE 6 or 2Africa. The downsides to the consortium model include the

⁴ These statistics reflect Recorded Future analysis of TeleGeography's [Submarine Cable Map](#).

need to [balance](#) the individual priorities and management approaches of multiple stakeholders, the likelihood of involvement by state-owned enterprises, and the challenges of satisfying numerous government regulators.

The growing role of hyperscalers as primary or joint owners of cables connecting underserved markets [raises](#) concerns over market monopolies and digital sovereignty. The power imbalance that accrues to these cable owners as a result will likely shape domestic policy considerations in these markets, most notably internet and data privacy regulations. Google and Meta, which have each undertaken major projects to connect Africa with the rest of the world, will have the technical ability (and may have the commercial pressure) to prioritize their respective platforms — such as Facebook, Instagram, WhatsApp, and YouTube — and associated content amid the torrent of data flowing into the continent. The implications for African societies and political structures could be far-reaching. For example, local African governments may find themselves with reduced leverage when attempting to press Google and Meta to adopt enhanced content moderation of their social media platforms, a critical issue given that disinformation has been [spread](#) on these platforms [across](#) Africa.

More Options, New Imperatives for Physical Security Attacks and Exploits

Recent major geopolitical developments — including Russia's 2022 invasion of Ukraine, China's increasingly [coercive](#) approach to seeking unification with Taiwan, and the continued [decline](#) in US-China relations — have created new imperatives for countries to conduct physical security attacks to disrupt cable system operations and covertly tap into the data flowing through them for national security and economic espionage purposes.

Cutting the (Underwater) Cord

State actors almost certainly represent the most significant threat for targeted physical security attacks on submarine cables, based on intentions, capabilities, and impact. They are the most likely to possess the specialized expertise and equipment to identify and sever a cable in deepwater, where it would cause the greatest disruption and achieve a strategic outcome. Technically simple attacks by non-state actors — such as a 2013 [attempt](#) by 3 divers to cut the [SEA-ME-WE 4](#) submarine cable off the coast of Alexandria, Egypt — can create short-term, costly disruptions, but they are very likely to take place closer to shore, where the damage is more readily repaired. Illustrating this point, unknown attackers [cut](#) submarine cables in Marseille, France, twice in 2022, but the cables were quickly [repaired](#) since the location of the damage was onshore.



Figure 6: Damaged submarine cables in manhole near Marseille landing station (Source: [Social Media](#))

Russia's full-scale invasion of Ukraine in February 2022, and China's ongoing [preparations](#) for unification with Taiwan — which may include the use of force — have significantly altered the geopolitical threat landscape for submarine cables, creating new incentives for Moscow and Beijing to disrupt or sabotage them. Currently, Russia almost certainly represents the most likely direct threat to the physical security of submarine cables, particularly those in the North Sea region, [aligned](#) with its hybrid warfare strategy. In the event of an invasion of Taiwan, China, which is already the source of numerous incidents [damaging](#) submarine cables connected to the island, would also very likely [present](#) an even greater direct threat to submarine cables in the immediate region. This assessment is predicated on the assets each country can deploy — specifically stealth submarines, submersible craft, maritime militia, or specialized surface vessels capable of reaching cables in deep sea locations — and credible evidence linking them with operational activity targeting cables.

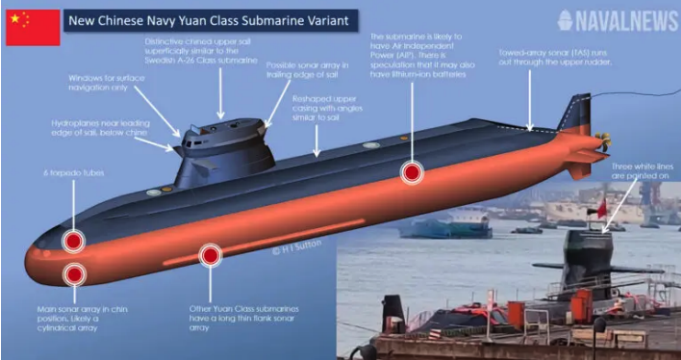

China	
Current Stealth Submarine/Submersible/Surface Vessel Fleet	
<ul style="list-style-type: none">Type-039C (Source: 1, 2, 3)	 <p>The diagram shows a side profile of a submarine with several callouts: 'New Chinese Navy Yuan Class Submarine Variant' (top left), 'Electric line (cable) upper sail' (top), 'Window for surface navigation only' (top), 'Hydroplanes near leading edge of sail, beam chine' (top), 'A-keppa tubes' (top), 'Main sonar array in chin position, likely a cylindrical array' (bottom left), 'Forward sonar array in leading edge of sail' (top), 'Redesigned upper casing with angles similar to sail' (top), 'This submarine is likely to have an Independent Power (AP), there is speculation that it may also have lithium-ion batteries' (top right), 'Towed-array sonar (TAS) runs out through the upper hull' (top right), and 'These white lines are painted on' (bottom right). The source 'NAVALNEWS' is in the top right corner.</p> <p>Figure 7: New China submarine, Type-039C (Source: Naval News)</p>
<ul style="list-style-type: none">Maritime militia/civilian fleet (Source: 1, 2, 3)	 <p>An aerial photograph showing a large number of blue and white fishing vessels with red flags, sailing in formation on the water.</p> <p>Figure 8: Chinese civilian fishing vessels (Source: Military Review)</p>
Credible Links to Cable Sabotage	
<ul style="list-style-type: none">Feb. 2023: 2 submarine cables connecting Taiwan with the outlying island of Matsu were cut by Chinese civilian ships — likely intentionally — within 6 days of each other. According to Taiwan authorities, cables linking Taiwan and its outer islands have been damaged 30 times since 2020, either accidentally or on purpose.	

Table 2: Breakdown of China's capabilities and credible linkages to submarine cable sabotage
(Source: Recorded Future)

Russia

Current Stealth Submarine/Submersible/Surface Vessel Fleet

- *Belgorod* (K-329)
(Source: [1](#), [2](#))



Figure 9: Belgorod K-329 submarine (Source: [Naval News](#))

- *Losharik* (AS-31)
(Source: [1](#), [2](#), [3](#))

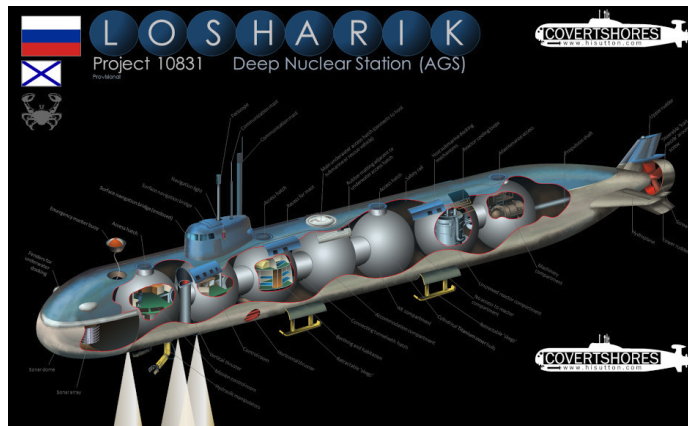


Figure 10: Losharik AS-31 submarine (Source: [Covert Shores](#))

- *Podmoskovye* (BS-64)
(Source: [1](#), [2](#))

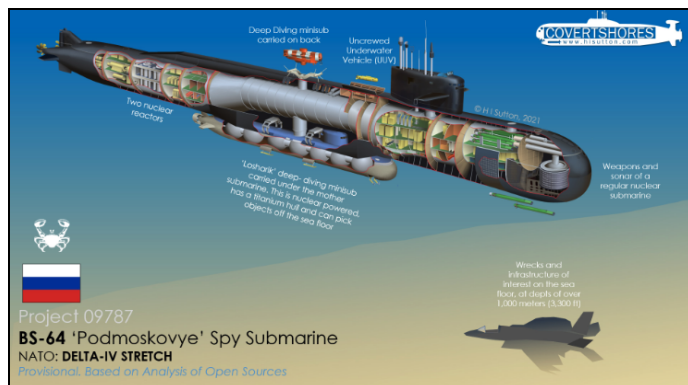


Figure 11: Podmoskovye BS-64 submarine (Source: [USNI News](#))


<ul style="list-style-type: none">Yantar (Source: 1, 2, 3)	 <p>Figure 12: Yantar surface vessel (Source: BBC)</p>
Credible Links to Cable Sabotage	
<ul style="list-style-type: none">Feb. 2023: A member of the United Kingdom’s Royal United Services Institute claimed Russia is likely developing special-purpose submarines to target submarine cables and other infrastructure.Feb. 2023: A joint Dutch Military Intelligence and Security Service-General Intelligence and Security Service report stated Russia is undertaking preparations for sabotaging offshore infrastructure in the North Sea, such as submarine cables, gas pipes, and windmill farms.Sept. 2022: A Danish patrol boat identified a Russian naval vessel, which carries a small submersible designed for underwater operations, in the vicinity of the Nord Stream gas pipelines several days before they were destroyed.Jan. 2022: The head of the UK’s Armed Forces stated, “Russia has grown the capability to put at threat those undersea cables” that represent the “world’s real information system”.Jan. 2022: Norway’s government reported that a submarine cable connecting its mainland to the Svalbard archipelago was severed, which law enforcement investigators determined to be the result of “human impact”.	

Table 3: Breakdown of Russia’s capabilities and credible linkages to submarine cable sabotage
(Source: Recorded Future)

On average, there are over 100 submarine cable faults each year: instances in which the cables are [damaged](#) or severed entirely, interrupting their ability to transmit data. The majority of physical damage to cables is accidental, often occurring as a result of fishing vessels trawling the ocean or ships dragging their anchors across the seabed. Geological events occur much less frequently, but their impacts can be more consequential. The January 2022 volcanic eruption off the coast of Tonga [caused](#) multiple faults in the 2 cables servicing the island nation, cutting off nearly all of its internet access for over a month.

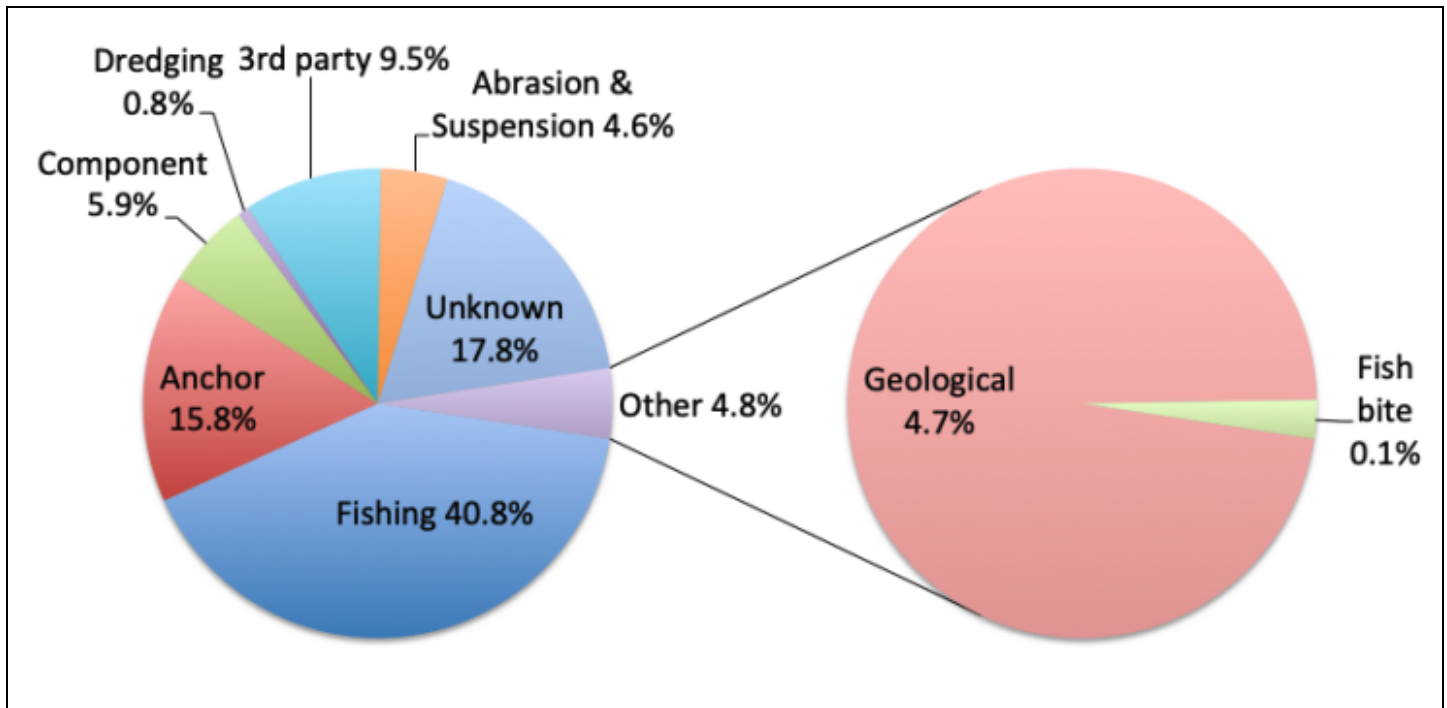


Figure 13: Causes of cable faults, 1959 to 2021 (Source: [International Cable Protection Committee](#))

While much less frequent, intentional damage or sabotage represents a unique threat vector, since the timing of an attack and target can disproportionately affect the countries and companies that rely on that cable system. Tonga's reliance on a single fiber-optic connection to the internet resulted in a catastrophic loss of connectivity, for example. In instances involving suspected intentional attacks, such as repeated [severing](#) of the submarine cables connecting Taiwan with its outlying island of Matsu over the past 5 years, the impact has been more manageable — slower internet connections and dropped phone calls — but the larger message was unmistakable: undersea data lifelines are vulnerable to disruption at a time and place of the attacker's choosing.

Intentional targeting of submarine cables in physical security attacks is not new. During the 1898 Spanish-American War, the USS Zafiro [cut](#) the cable connecting Manila, Philippines, to Hong Kong, creating an information disadvantage for rival Spanish forces based there. In the early stages of World War I less than 2 decades later, the UK [crippled](#) Germany's ability to communicate across the world by dredging up and sabotaging its telegraph cables. More recently, in 2015, US national security officials [raised](#) alarms over the physical security threat posed by Russian submarines maneuvering near cables from the North Sea to Northeast Asia, and the Russian ship *Yantar* operating near American shores. And in 2017, an unknown actor severed and removed 2.5 miles of cable [connecting](#) elements of Norway's underwater submarine surveillance network — an act that had relatively limited impact outside of the Institute of Marine Research, which owns and operates the network, but made it easier for submarines to pass undetected through this key northern waterway.

The increasing volume and sensitivity of the data [transmitted](#) along submarine cables today, however, and their centrality to global finance, has amplified the impact posed by a physical security attack. As a

diverse array of providers and sectors [embrace](#) cloud computing, they (and their customers) have become more [reliant](#) on low latency, high-quality solutions. The widespread [growth](#) of 5G, particularly in Africa, will almost certainly further reinforce this dependency.

Tapping Into Information Superhighways

For countries intent on gleaning insights to strengthen their national security or achieve an economic advantage, submarine cables [represent](#) a wealth of information. Underwater intelligence collection has a long history — most notably Operation Ivy Bells, a Cold War-era operation in which the US [tapped](#) into a key Soviet Union military communication cable in the Sea of Okhotsk. The rapid growth of submarine cable systems has [created](#) significantly more opportunities to [tap](#) into these underwater information superhighways, with the most vulnerable [targets](#) very likely the landing stations where they come ashore.

The challenge in recreating Operation Ivy Bells today is the sheer magnitude of data coursing through submarine cables — capable of [reaching](#) 250 terabytes per second — and the need to establish a mechanism for filtering or transferring it to land-based analysts from its underwater location. According to some [observers](#), this is a prohibitively difficult task. It is likely that only a select few countries are [capable](#) of [tapping](#) into submarine cables in deepwater locations, where their activities are less likely to be detected. Landing stations therefore present a more readily accessible option.

Despite their importance in the submarine cable ecosystem, landing stations are often nondescript, low-security buildings, primarily [chosen](#) for their proximity to a carrier, data center, or point of presence (POP). The [operators](#) of these facilities can be a local telecommunications company, the submarine cable owner, or an international consortium. [Security](#) for these facilities vary widely, even in advanced economies. The Africa Coast to Europe cable landing station outside Freetown, Sierra Leone, for example, features a small, walled-in [compound](#) in close proximity to a nearby neighborhood.



Figure 14: Cable landing station outside Freetown, Sierra Leone
(Planet SkySat: Powered by Planet: SkySat 50cm. Courtesy of SkyWatch)

Access to these cables where they come ashore is not always well secured, a vulnerability that is exacerbated by the practice of running multiple cables along similar routes, [creating](#) significant chokepoints. The 2022 cable severing incidents in Marseille, where 16 cables currently land or are confirmed to land in the near future, illustrated this point. It is very likely that an intelligence collection operation by a state actor would make similarly productive use of such a low-security access point. In some instances, it may be most effective to use a physical attack to [drive](#) data traffic onto a compromised cable.

Landing stations can [serve](#) as intelligence collection points by their owners, on behalf of their country or for the benefit of a foreign government, through the insertion of monitoring equipment or backdoor software. The present or perceived risk of intelligence operations targeting landing stations is illustrated by 3 recent examples:

- The government of Mauritius is currently embroiled in [controversy](#) amid allegations that its prime minister pressured Mauritius Telecom to allow the [installation](#) of internet “sniffing” capabilities at the Baie Jacotet landing station on behalf of Indian intelligence.
- David Panuelo, the outgoing president of the Federated States of Micronesia, [asserted](#) in a recent letter that China had pushed on multiple occasions to sign a Memorandum of Agreement, which would have granted Beijing control of the country’s submarine cables and telecommunications infrastructure.
- In 2021, a US government interagency committee [recommended](#) denial of a license application to create a new landing station for the ARCOS-1 cable system in Cuba, citing espionage-related concerns over the involvement of Cuba’s state-owned telecommunications provider, Empresa de Telecomunicaciones de Cuba S.A. (“ETECSA”).

Encryption [remains](#) the primary defense against spying on submarine cables, which will very likely limit the threat actors capable of exploiting this data. Despite concerns that [advances](#) in quantum computing may soon crack the encryption code, ongoing research suggests quantum computing may also provide tools for maintaining effective defenses. In 2019, researchers successfully [tested](#) quantum key distribution, which uses entangled photon pairs to secure communication, over a 96-kilometer segment of submarine cable. And in 2020, Microsoft used post-quantum cryptography to [secure](#) an encrypted network tunnel connecting to an underwater data center.

Network Management Vulnerabilities

In an effort to reduce costs, streamline operations, and enhance performance, submarine cable owners and operators are increasingly [turning](#) to remote network management systems to monitor and control their infrastructure. These systems almost always require connection to the internet, exposing them to state-sponsored adversaries, ransomware groups, hacktivists, and other cyber threat actors. The pursuit of expediency can therefore have very significant costs, as third-party vulnerabilities become more likely to jeopardize the security and resilience of the entire cable system. A glimpse of that possible future occurred in April 2022, when federal authorities thwarted a [cyberattack](#) against a submarine cable operating system in Hawaii, enabled by a credentials-related breach of a third-party.

Previously, on-site system monitoring tools were responsible for [managing](#) equipment related to submarine line terminals and power feeds. The advent of more complicated cable systems incorporating new technological advances has led to the adoption of remote network management systems by providers such as Ciena or NEC Corporation. As industry [approaches](#) the Shannon limit — a 1948 theory that [posits](#) there is a maximum rate at which data can be transmitted through a communication channel before errors creep in — it has become more vital to increase bandwidth capacity by improving the efficiency of data flows. The new network management systems enable operators to control essentially all elements of a submarine cable system to that end, including their “physical and optical layer, line terminal equipment, repeaters, branching units, landing stations and other network operation centers, even those residing in other nations”.⁵ New vendor offerings [boast](#) of cloud-native platforms using open APIs, capable of visualizing foreign line systems and third-party internet infrastructure.

The cost savings and performance enhancement capabilities offered by remote network management systems can come at a cost of increased risk, however. They [rely](#) on internet connectivity bridging them to the cables, open-source software, and operating systems, such as Windows and Linux, with which cyber threat actors are well-acquainted at exploiting ([1](#), [2](#)). Major cyberattacks that have exploited vulnerabilities in remote management systems or similar products in recent years include the 2020 [breach](#) of SolarWinds' Orion platform and the 2021 [breach](#) of Kaseya's Virtual Systems Administrator product. These attacks highlight the risk involved in the use of third parties, especially if the compromised products occupy privileged positions on customer networks.

⁵ Michael Sechrist, “New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems” p. 12. Belfer Center Discussion Paper, No. 2012-03, Harvard Kennedy School, February 2012.

Outlook

If data is the lifeblood of today's digitized world, then submarine cables are the critical arteries that sustain it. With no viable alternative on the horizon, the importance of these underwater conduits to global finance, national security, and international communications will almost certainly increase as the demand for data accelerates. The continued growth of the submarine cable network, fueled by hyperscalers, and efforts to maximize efficiency through network management systems, will very likely ensure that this demand will be met, but it will also introduce new complexities and opportunities for threat actors to exploit.

In the wake of Russia's war against Ukraine, China's ongoing preparations for unification with, and coercion of, Taiwan, and a deepening US-China divide, the geopolitical risk environment for submarine cable owners and operators — and the countries and companies that rely upon them — will very likely deteriorate in the near term, resulting in heightened risk for state-sponsored physical and cybersecurity attacks. The impact of these attacks will vary widely, ranging from intermittent traffic disruptions to widespread outages that take days or weeks to resolve, depending on the redundancy and resiliency of the affected network.

State actors seeking an espionage edge will almost certainly target the entire submarine cable ecosystem for intelligence collection: landing station infrastructure, the submarine cables themselves, third-party providers, and the hardware and software that knits it all together. Separately, Russia will almost certainly increase its overt and covert mapping of submarine cables, and likely engage in targeted sabotage on land and underwater, to inconvenience western countries, as well as determine utility for hybrid warfare applications. China will also very likely continue to probe and disrupt the cables Taiwan relies upon.

Non-state actors, including hacktivists and ransomware groups, will likely pose a less capable and lower likelihood threat to the networks and operating systems that submarine cables rely upon, but their threat cannot be discounted. Accidental damage from ship anchors or fishing vessels will also remain higher likelihood, but lower impact events.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture