Undersea Telecommunication Cables: Technology Overview and Issues for Congress

September 13, 2022

Congressional Research Service
https://crsreports.congress.gov
R47237

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47237

September 13, 2022

Jill C. Gallagher
Analyst in Telecommunications Policy

Undersea Telecommunication Cables: Technology Overview and Issues for Congress

Undersea telecommunication cables enable consumers, businesses, and governments, including the military, to communicate with each other and to access the internet. Private and state-owned telecommunication and technology companies operate about 486 undersea telecommunication cables, which connect every continent except Antarctica. These privately owned cables carry about 99% of transoceanic digital communications (e.g., voice, data, internet), including trillions of daily international financial transactions, and serve as the backbone for the global internet.

Recent damage and threats to commercial undersea telecommunication cables have raised concerns among U.S. officials and experts over the security of commercial undersea telecommunication cables. In January 15, 2022, a volcanic eruption and earthquake in Tonga severed its only connection to the internet. Repair crews restored service to the main island within several weeks; however, the cable connecting Tonga's 170 outer islands to the main island and to each other is still under repair, leaving people and businesses in those areas without service. The outage of its sole cable disrupted Tonga's communications, recovery efforts, and financial markets, including remittances from abroad on which many families depend. Russia's invasion of Ukraine has also increased concern about the security of commercial undersea telecommunication cables among some North Atlantic Treaty Organization (NATO) nation leaders, given previous reports of Russian capabilities to cut or tap undersea cables and its activities near NATO nations' undersea infrastructure. The U.S. Department of Justice raised issues related to commercial undersea cables connecting the United States to China, citing increased potential for the Chinese government to access undersea cable systems to obtain personal information, data, and communications. Finally, a cyberattack on a commercial undersea telecommunication cable connecting Hawaii and the Pacific region has raised awareness and concern among U.S. officials on the cybersecurity of commercial undersea telecommunication cables.

The U.S. government has studied security of commercial undersea telecommunication cables in the past. A 2017 report sponsored by the Office of the Director of National Intelligence (ODNI) found that the majority of disruptions are caused by human activity (e.g., fishing, anchoring, dredging) and natural disasters. The ODNI report found there are few disruptions of cables in proportion to their heavy presence and use. Automated detection systems, increased redundancy of routes, and a network of repair ships has led to a high degree of resiliency in the global undersea cable network. However, the ODNI report asserted that risks are increasing, due to the heavy reliance on undersea cables, increasing volume of data transmitted through undersea cables, and technological improvements to cable systems that have created new vulnerabilities. The Communication Security, Reliability and Interoperability Council (CSRIC)—a federal advisory committee to the Federal Communications Commission (FCC)—issued a series of reports identifying risks to cables and recommendations for strengthening the security and resiliency of commercial undersea telecommunication cables. The CSRIC identified a need for a lead agency to improve coordination among U.S. government agencies involved in reviewing cable landing applications; increase coordination between the U.S. government and private sector owners to establish and promote protection standards (e.g., protection zones, spatial separation standards); and promote participation in international organizations aimed at protecting undersea telecommunication cables.

The U.S. government has acted to protect undersea telecommunication cables and the U.S. telecommunication network. It has strengthened processes for reviewing foreign ownership interest of cables landing in the United States; restricted the use of untrusted equipment in undersea cable systems; encouraged investment in trusted equipment in the United States and abroad; established an outage reporting system for undersea cables; and expanded its cable repair fleet. Some have called for a more coordinated approach to securing undersea cables such as appointing a lead agency to oversee cable security or establishing a public-private initiative to enhance cable security. On the one hand, these are private assets, maintained by their owners, with few disruptions reported. On the other hand, given the heavy reliance on commercial undersea cables for consumer, financial, government, and some military communications, and given the increasing threats from human activity, natural disasters, and bad actors, Congress may increase U.S. government oversight and involvement in ensuring security of commercial undersea telecommunication cables.

This report discusses the technology of undersea telecommunication cables, threats to cables, U.S. government actions to protect cables, and issues for congressional consideration.

Contents

Introduction 1
Undersea Telecommunication Cable Systems 2
Dry Plant 5
Cable Landing Station 5
Beach Manhole 6
Wet Plant 6
Fiber-Optic Cable 6
Recent Technical Developments 8
Threats to Undersea Telecommunication Cables 9
Unintentional Damage to Cables 9
Human Activities 10
Natural Disasters 10
Intentional Damage to Undersea Telecommunication Cables 11
Repairing Damaged Undersea Telecommunications Cables 12
Cyberattacks 13
U.S. Actions to Protect Cables 13
Foreign Ownership Review 14
Restrict Use of Untrusted Equipment 15
Facilitate Investment in Trusted Equipment 16
Enhance Cable Security Review 17
Monitor Cable Outages 18
Identify Policies and Standards to Protect Cables 18
Invest in Cable Repair Vessels 18
Issues for Congress 19
Role of U.S. Government in Protection of Cables 19
Connections with Adversarial Nations 20
Restrictions on Technologies or Technology Firms 21
Strengthening Security Requirements 21
Addressing the Risk of Damage Through Commercial Activity 21
Conclusion 21

Figures

Figure 1. Map of Commercial Undersea Telecommunications Cables 4
Figure 2. Undersea Telecommunication Cable System 5
Figure 3. Undersea Fiber-Optic Cable Cross-Section 7
Figure 4. Cause of Undersea Telecommunication Cable Faults (1959 to 2021) 10

Contacts

Author Information 22

Introduction

Telecommunications providers have used undersea cables (also known as submarine or subsea cables) for long-distance communications for more than 170 years. The English Channel Submarine Telegraph Company laid the first undersea cable in 1850 between England and France, to enable international communications over telegraph.

The first successful transatlantic telegraph message carried by undersea cable was transmitted in 1858, the first transatlantic telephone cable entered operation in 1956, and the first transatlantic fiber-optic cable was laid in 1988.[1] The fiber-optic cable, called the TAT-8, had the capacity to carry 40,000 telephone connections simultaneously, four times the capacity of previous cables.[2] One telecommunication market research and consulting firm that maps undersea cables, estimates that, as of April 2022, there are 486 commercial undersea telecommunication cable systems and 1,306 landing stations (i.e., the point where the undersea cable makes landfall) currently active or under construction.[3] The cables connect every continent except Antarctica,[4] and serve as the backbone for the global internet.[5] Industry experts estimate that the undersea telecommunication cable network carries about 95% of intercontinental global internet traffic,[6] and 99% of transoceanic digital communications (e.g., voice, data, internet),[7] including trillions in international financial transactions daily.[8]

With the proliferation of mobile phones and other devices that connect wirelessly to telecommunication networks, and the global expansion of those networks, demand for mobile data is increasing. One industry report estimates that in 2020, amid the COVID-19 pandemic, the global market for mobile data traffic was 47.6 million terabytes per month; the report projects it to reach 220.8 million terabytes per month by 2026, growing at a compound annual growth rate of 28% over the analysis period.[9] The growth is driven in large part by video use, as well as the

[1] Mischa Schwartz and Jeremiah Hayes, "A History of Transatlantic Cables," *IEEE Communications Magazine*, vol. 46, no. 9 (September 12, 2008), pp. 42-48, https://ieeexplore.ieee.org/document/4623705; Gerard Fouchard, "Historical Overview of Submarine Communication Systems," in *Undersea Fiber Communication Systems*, ed. Jose Chesnoy, 2nd ed. (London: Academic Press, 2016).

[2] CBR Staff Writer, "Fibre Optic TAT-8 Cable Goes into Service across the Atlantic," *Tech Monitor*, December 15, 1988, https://techmonitor.ai/techonology/fibre_optic_tat_8_cable_goes_into_service_across_the_atlantic.

[3] Jayne Miller, "Two New Maps, Lots of New Cables," *TeleGeography* (blog), April 4, 2022, https://blog.telegeography.com/two-new-maps-lots-of-new-cables.

[4] TeleGeography, "Submarine Cable Frequently Asked Questions: Submarine Cable 101," https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

[5] Brian E. Carpenter, *Network Geeks: How They Built the Internet* (London: Springer Science & Business Media, 2013), p. 80.

[6] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council Scowcroft Center for Strategy and Security, September 13, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.

[7] Christian Bueger and Tobias Liebetrau, "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network," *Contemporary Security Policy*, vol. 42, no. 3 (2021), pp. 391-413, https://www.tandfonline.com/doi/full/10.1080/13523260.2021.1907129.

[8] The International Cable Protection Committee, *Submarine Cables and BBNJ (Biodiversity in areas Beyond National Jurisdiction)*, 2016, p. 1, https://www.un.org/depts/los/biodiversity/prepcom_files/ICC_Submarine_Cables_&_BBNJ_August_2016.pdf; see also Maritime Awareness Project, "Factsheet: Submarine Cables," https://map.nbr.org/2018/07/submarine-cables/.

[9] Global Industry Analysts, Inc., "New Analysis from Global Industry Analysts Reveals Steady Growth for Mobile Data Traffic, with the Market to Reach 220.8 Million Terabytes per Month Worldwide by 2026," *PR Newswire*, December 8, 2021, https://www.prnewswire.com/news-releases/new-analysis-from-global-industry-analysts-reveals-

expansion of data center and cloud services—especially intensive data communications for large-scale distributed data storage, management, and process—made available to companies by cloud computing service providers (e.g., Amazon, Microsoft, Google). Increase in demand for these services has driven demand for additional cables with increased capacity.[10]

Recently, some national security observers have called attention to the importance of commercial undersea telecommunication cables, and recommended greater U.S. government involvement in cable planning to protect cables from unintentional and intentional damage, and to prevent foreign adversaries from accessing communications and data transmitted through cables.[11] The recommendations overlap those made in a 2017 report sponsored by the Office of the Director of National Intelligence (ODNI)[12] and by the advisory committee to the Federal Communications Commission (FCC) in a series of reports on undersea cable security and resiliency, issued from 2014 through 2016.[13] Recommendations include physical protection policies, public-private cooperation on cable security, education, and international engagement to protect commercial undersea telecommunication cables from damage and espionage. With the emergence of fifth-generation (5G) telecommunications technologies, Congress has shown an interest in protecting U.S. and global terrestrial (land-based) telecommunication networks.[14] Given the importance of commercial undersea cables for carrying 5G and internet data traffic, Congress may also focus on the security of undersea cables and the data they carry, and the role of the U.S. government in protecting these privately-held assets.

This report provides an overview of undersea telecommunication cable technologies, threats to undersea telecommunication cables (unintentional and deliberate damage), and U.S. government actions to protect cables. The report concludes with issues for congressional consideration, including additional federal policies and measures to protect cables such as restricting landing cables in the territory of nations deemed to be adversaries; restricting the use of equipment from firms in nations deemed to be adversaries; and policies to mitigate threats to and strengthen the security and resiliency of commercial undersea telecommunication cables.

Undersea Telecommunication Cable Systems

When people communicate using wired or wireless digital devices, the information they send often traverses multiple interconnected telecommunication service networks before reaching the intended recipient. Telecommunication and internet service providers use high-capacity terrestrial (land-based) networks to carry communications within contiguous landmasses. However, to

steady-growth-for-automotive-ethernet-with-the-market-to-reach-4-9-billion-worldwide-by-2026—301576778.html.

[10] Stephanie Wong, "Google's Subsea Fiber Optics, Explained," *Google* (blog), April 6, 2022, https://cloud.google.com/blog/topics/developers-practitioners/googles-subsea-fiber-optics-explained (Stating "Cloud is a big growth driver of Google's network demand, with Gartner predicting the world's cloud spending to increase to $917B by 2025.")

[11] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council Scowcroft Center for Strategy and Security, September 13, 2021; see also Jonathan E. Hillman, *Securing the Subsea Network, A Primer for Policymakers*, Center for Strategic and International Studies, A Report of the CSIS Reconnecting Asia Project, March 2021, https://www.csis.org/analysis/securing-subsea-network-primer-policymakers.

[12] ODNI, *Threats to Undersea Cable Communications* (ODNI Report), September 28, 2017, https://www.dni.gov/files/PE/Documents/1—2017-AEP-Threats-to-Undersea-Cable-Communications.pdf.

[13] The reports are available at FCC, "Communications Security, Reliability, and Interoperability Council (CSRIC), Reports," https://www.fcc.gov/CSRICReports.

[14] For further details, see CRS Report R47012, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests*, by Jill C. Gallagher.

transmit communications between landmasses separated by large expanses of water, telecommunication and internet service providers rely on undersea telecommunication cables. Providers transmit voice and data communications through their terrestrial networks in the originating geography through an undersea cable to a terrestrial network in the terminating geography, which carries them to the intended recipients.[15]

Telecommunication companies (e.g., AT&T, Verizon, Deutsche Telekom, China Mobile), own and operate most undersea cables.[16] One company or a consortium of companies may own a single commercial undersea telecommunication cable. In the late 1990s, consortia of companies and investors built undersea cables and sold the capacity to carriers. According to a report from one policy think tank, single-owner entities own around 65% of the undersea telecommunication cables, while consortia own 33%.[17] Starting around 2015, technology companies, such as Google,[18] Facebook, and Amazon, began investing in and building their own undersea cables, as sole owners or as parts of a consortium, to meet increasing demands.[19]

In the United States, as well as in many other nations, repair and maintenance of commercial undersea telecommunication cables is primarily a private sector responsibility. Cable owners may develop agreements between themselves and with other infrastructure owners (e.g., offshore power transmission cable and pipeline owners). These private agreements could define the placement of the respective infrastructures; crossing notification procedures, where owners agree to install cables at minimum distances apart in locations where a cable may cross an existing undersea telecommunication cable or other infrastructure; and access agreements for maintenance and repair, to avoid harm to cables.

Figure 1 shows the geographic distribution of undersea telecommunication cables in June 2022.[20]

[15] Bryan Clark, "Undersea Cables and the Future of Submarine Competition," *Bulletin of the Atomic Scientists*, vol. 72, no. 4 (2016), p. 234, https://www.tandfonline.com/doi/pdf/10.1080/00963402.2016.1195636.

[16] TeleGeography, "Submarine Cable Frequently Asked Questions: Submarine Cable 101," https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

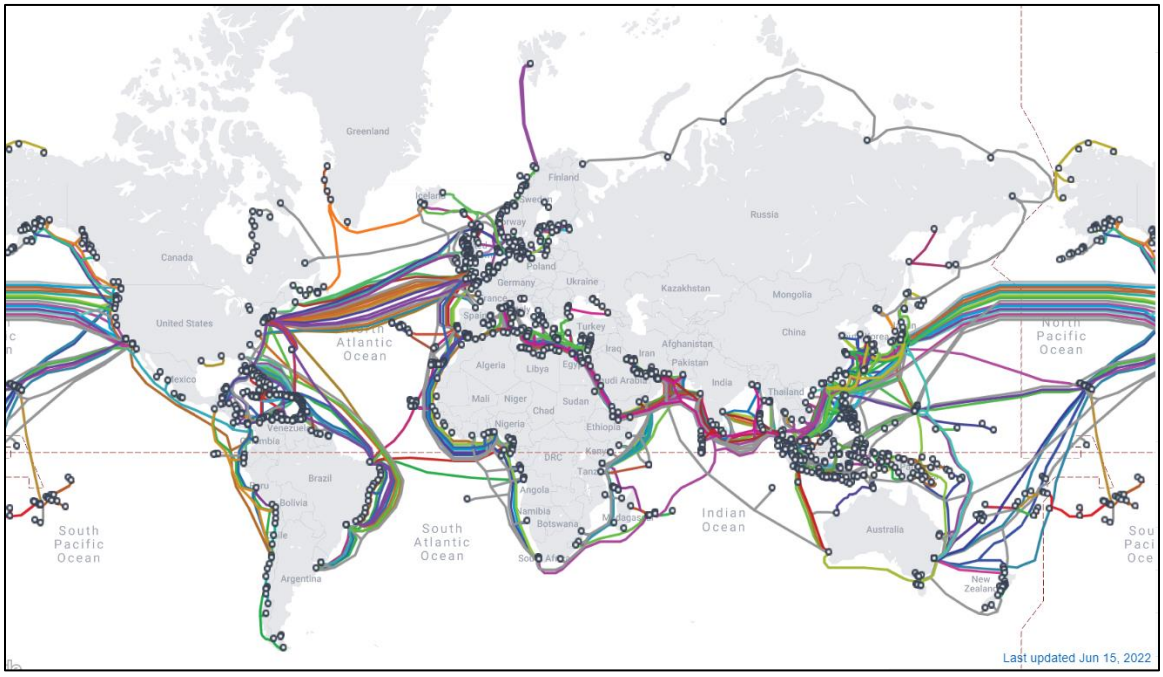
[17] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council Scowcroft Center for Strategy and Security, September 13, 2021. (Note: Total ownership does not add up to 100% because ownership of some cables was not provided to or coded by TeleGeography, the author's data source.)

[18] In 2015, Google formed a parent company named Alphabet; Google is the largest wholly owned subsidiary of Alphabet.

[19] Alan Mauldin, "A Complete List of Content Providers' Submarine Cable Holdings," TeleGeography Blog, November 9, 2017 (updated 2020), https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list. There are many types of technology firms such as internet service providers (e.g., AT&T, Comcast), content providers or over-the-top providers (e.g., Netflix, Hulu), hyperscalers or web-scale companies (e.g., Google, Apple, Facebook, Microsoft, and Amazon), cloud service providers (e.g., Amazon, Microsoft, Google, and IBM), etc. TeleGeography uses the term "content providers" but notes that the top four investors—Google, Facebook, Amazon, and Microsoft—are hyperscalers.

[20] The map shows commercial undersea telecommunication cables, and does not include many government-owned cables. For example, the U.S. Navy operates about 40,000 miles of undersea cables. For awareness, there are other types of cables, such as undersea power cables, which provide electric power transmission service across regions.

Figure 1. Map of Commercial Undersea Telecommunications Cables

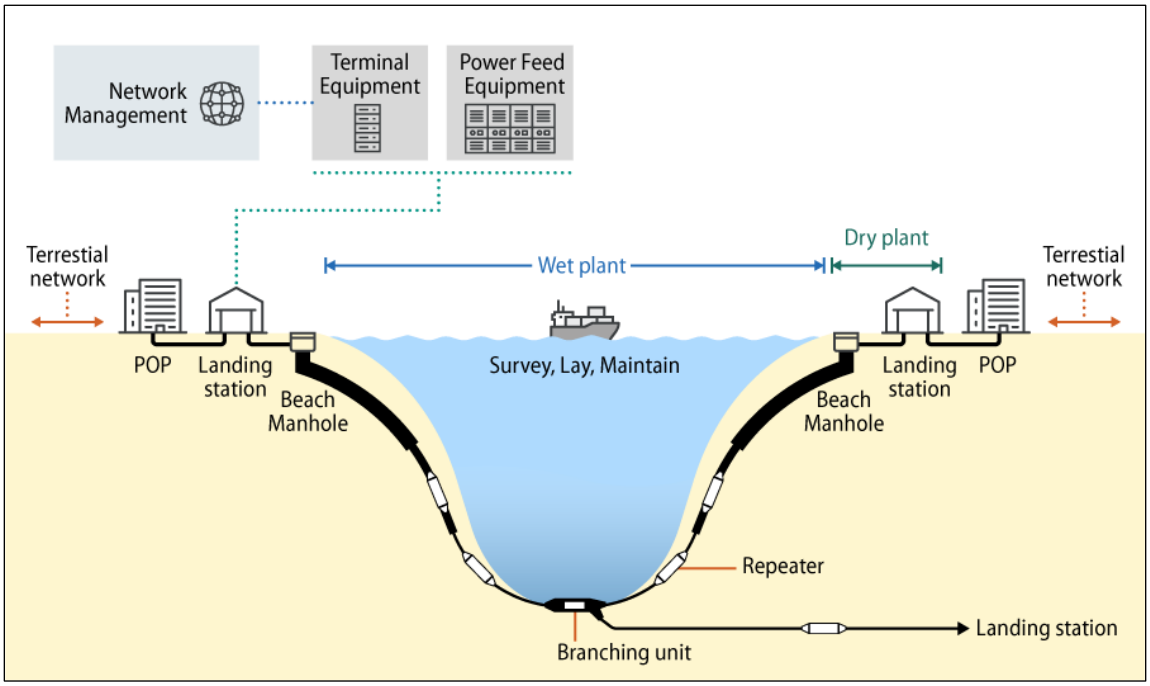


Source: TeleGeography, *Submarine Cable Map*, 2022, https://www.submarinecablemap.com/.

Note: Geographic distribution of commercial undersea telecommunication cables as of June 15, 2022. Colors are used in the figure to visually differentiate undersea telecommunication cables in close proximity to one another. Colors may repeat in different geographic areas. The hollow circles signify cable landing stations. This map shows both domestic and international undersea telecommunication cables. Domestic undersea telecommunication cables lay point to point within a country to improve connectivity between regions within a country, and provide connectivity to the global internet. Some domestic cables cross into international waters when connecting two domestic points. International cables connect two or more countries; these enable connection between the countries and to the global internet. This map shows commercial cables and does not include all government-owned cables, such as those used for military and intelligence purposes.

An undersea telecommunication cable system includes two or more onshore terminal stations (or cable landing stations) connected by a fiber-optic cable. The cable landing stations contain transmission, reception, and network management equipment. The fiber-optic cable may include repeaters within the cable that boost transmitted signals and branching units that allow a cable to serve multiple end-points (**Figure 2**).

Figure 2. Undersea Telecommunication Cable System



Source: Created by CRS.

Note: Graphic shows an undersea telecommunication cable system, including cable landing stations and equipment (e.g., terminal equipment and power feed); undersea cable (with repeaters, and a branching unit) running from beach manhole to beach manhole; and fiber lines from the cable landing station to a point-of-presence that connects via fiber to inland terrestrial networks. POP=point-of-presence.

The following sections provide more detail on the segments of a cable system, including fiber-optic cables, the terrestrial portion of an undersea telecommunication cable system called the "dry plant," and the undersea portion called the "wet plant."

Dry Plant

The dry plant is the terrestrial segment of an undersea cable system, running from a cable landing station to the beach manhole.[21] A cable landing station is typically a few hundred meters from the beach manhole near the shoreline and connected by a short, repeater-less fiber link.

Cable Landing Station

A cable landing station is an on-shore facility where undersea cables arrive and terminate.[22] Cable landing stations contain submarine line terminal equipment (SLTE) that can transmit and receive signals. They receive signals from the undersea cable and transmit signals inland to terrestrial networks, usually through a provider's point-of-presence (POP) or interconnection facility, and can receive signals from terrestrial networks and transmit them to undersea cables. Since a POP

[21] Communications Security, Reliability and Interoperability (CSRIC) Working Group 4A Submarine Cable Resiliency, *Final Report—Clustering of Cables and Cable Landings* (CSRIC WG4A—Final Report on Cable Landings), August 2016, p. 4, https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG4A_Final_091416.pdf.

[22] Harry Newton, *Newton's Telecom Dictionary*, 27th ed. (New York: Flatiron Publishing, 2013), p. 245.

could be hundreds of miles from the seashore, operators often use a longer fiber link with repeaters to connect to the cable landing station.[23]

To transmit signals, electronically controlled semiconductor lasers (laser diodes) transmit signals by modulating (i.e., pulsing) light and sending it into the optical fiber. To receive signals, semiconductor optical detectors receive the light from the fiber, modulate the signals to produce a corresponding electrical signal, and transmit the signal to a provider's POP or interconnection facility, which transmits the signal to the provider's terrestrial telecommunications network.

Cable landing stations may also contain network management systems that allow operators to monitor and control cable operations and traffic, and power feed equipment (PFE) that provides a constant direct electrical current through the cable to power repeaters.[24]

Beach Manhole

The beach manhole is a "concrete chamber, buried into the beach, or road behind the landing point, where the submarine cable is terminated and from where the [fiber cable and power cable] are routed to the [cable landing station]. Most manholes are designed to take more than one cable, most commonly two."[25] Fiber connects the cable landing station to a beach manhole, where it joins the undersea cable.

Wet Plant

The wet plant is the segment of the cable system that runs from a beach manhole on one landmass to a beach manhole on another. Installation of new cables often requires boring and trenching to place the manhole on or near the seashore and drilling beneath the beach to lay feeder pipes to carry cables into the water. Special cable-laying ships, often equipped with a plough to dig a trench in the seabed in which to lay cable, continue the installation from shore to shore.

Fiber-Optic Cable

Since the late 1980s, commercial undersea telecommunication cable owners have used optical fibers—thin, flexible, and highly transparent glass or plastic strands—to facilitate long-distance communications.[26] Optical fibers allow signals to be sent over long distances using light pulses instead of electricity, which, when compared with traditional copper lines, results in a clearer signal, less signal loss over long distances, greater bandwidth, and less electromagnetic

[23] Olivier Courtois and Caroline Bardelay-Guyot, "Architectures and Management of Submarine Networks," Section 9.3.5 in *Undersea Fiber Communication Systems*, 2nd ed. (London: Academic Press, 2016).

[24] Tomoyuki Kaneko, Yoshinori Chiba, and Kaneaki Kunimi, "Power Feeding Equipment for Optical Submarine," *NEC Technical Journal*, vol. 5, no. 1 (February 2010), pp. 28-32, https://mathscinotes.com/wp-content/uploads/2015/03/PowerStuff.pdf; see also E.T. Calkin, I. Golioto, and W. Schatz, et al., "SG Undersea Cable System: Undersea System Power," *Bell System Technical Journal*, vol. 57, no. 7 (September 1978), pp. 2497-2522.

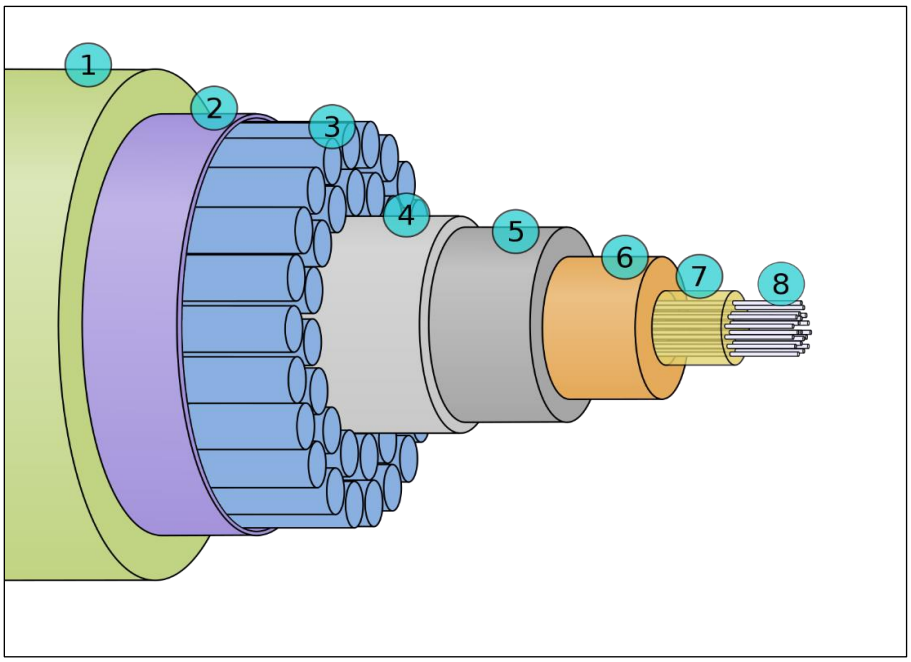
[25] CSRIC WG4A—Final Report on Cable Landings, p. 4.

[26] Earlier cables used copper wires to carry electrical signals; fiber-optic cables use light pulses to transmit digital data in a binary format.

interference.[27] Due to these advantages, network architects assert that optical fiber is the best physical medium to facilitate long distance communication and connect global networks.[28]

Optical fibers carry communications (e.g., voice, data, and internet) in the form of colored light signals of various wavelengths (using a technique known as wavelength division multiplexing)[29] to enable high-speed, long-distance communications.[30] The optical fibers themselves are encased in successive layers of materials to transmit power,[31] and to strengthen and insulate the cable. **Figure 3** illustrates the bundled materials in a typical undersea fiber-optic cable.

Figure 3. Undersea Fiber-Optic Cable Cross-Section



Source: Oona Räisänen, *Submarine Cable Cross-Section 3D Plain,* Public Domain, accessed November 30, 2021, https://commons.wikimedia.org/wiki/File:Submarine_cable_cross-section_3D_plain.svg.

Notes: (1) Polyethylene, (2) Mylar tape, (3) Stranded metal (steel) wires, (4) Aluminum water barrier, (5) Polycarbonate, (6) Copper or aluminum tube, (7) Petroleum jelly, and (8) Optical fibers.

[27] OptronicsPlus, *Fibre Optics vs Copper Cabling—Understanding the Difference*, White Paper, https://optronicsplus.net/downloads/whitepapers/OP_Fibre_Optics_vs_Copper_Cabling_Understanding_the_Difference_White_Paper_Rev.1.0.pdf.

[28] Alessandro Maggio, "Physical Layer: Fiber Optic Media, Data as Light Pulses," *ICTShore*, October 27, 2016, https://www.ictshore.com/free-ccna-course/physical-layer-fiber-optic-media/.

[29] In wavelength division multiplexing, multiple optical signals of different wavelengths (colors) are transmitted together across a single fiber-optic cable and separated again for further routing, thus increasing the data transmission capacity of the cable. See Charles A. Brackett, "Dense Wavelength Division Multiplexing Networks: Principles and Applications," *IEEE Journal on Selected areas in Communications*, vol. 8, no. 6 (August 1900), pp. 948-964; Klaus Grobe, "Wavelength Division Multiplexing," *Encyclopedia of Modern Optics*, ed. Bob D. Guenther and Duncan G. Steel, 2 ed. (Elsevier, 2018), pp. 255-290, https://www.sciencedirect.com/science/article/pii/B9780128035818094716.

[30] Jose Chesnoy, "Presentation of Submarine Fiber Communication," in *Undersea Fiber Communication Systems*, ed. Jose Chesnoy, 2nd ed. (London: Academic Press, 2016), p. 6.

[31] Michael Morris, "The Incredible International Submarine Cable Systems," *Network World*, April 19, 2009, https://www.networkworld.com/article/2235353/the-incredible-international-submarine-cable-systems.html. (Repeaters are powered by a constant direct current passed down a conductor near the center of the cable.)

Multiple fiber optic cores (segments 5-8 in **Figure 3**) can be combined within the outer insulation and strengthening layers (segments 1-4) of an undersea telecommunication cable. Near to the shore, the cable is wrapped in tough shielding to protect against danger and damage from activities occurring near to shore (e.g., fishing, shipping, and other marine activities).[32] Undersea cables can carry multiple fiber pairs, enabling numerous providers to use the same cable. Most cables transmit in one direction on one fiber in a pair and in the reverse direction on the other.[33] As optical signals pass from one segment of an undersea telecommunication cable to the next, repeaters boost the signal with optical amplifiers using semiconductor laser pumps, allowing the signal to travel long distances, and controlling the signal with optical equalizers to maintain its integrity.[34]

Recent Technical Developments

Advances in fiber optic undersea cable technologies—for transmitting, receiving, and boosting optical signals—have led average carrying capacity for undersea telecommunications signals to increase from 25 to 60 terabits per second (Tbps) between 2014 and 2019.[35] Recent technical developments—system designs to allow integration of faster network equipment, increasing the number of fiber pairs in a cable—have enabled undersea telecommunication cables to reach carrying capacities of up to 250 Tbps.

The MAREA undersea cable operating between Virginia Beach, VA, and Bilbao, Spain, can transmit up to 200 Tbps.[36] When it was completed in 2017, its owners—Microsoft, Facebook and Telxius (a subsidiary of Spanish telecommunications company, Telefónica)—stated that it was the "highest-capacity subsea cable to ever cross the Atlantic—featuring eight fiber-pairs and an initial estimated design capacity of 160 Tbps" operates "more than 16 million times faster than the average home internet connection."[37] MAREA used an open design, which allows for the integration of new, higher performing network equipment from a variety of makers into the existing cable system as it is developed.[38] In 2018, MAREA owners announced they had integrated new technologies into the system, increasing its capacity from 160 Tbps to 200 Tbps.[39]

[32] Doug Dawson, "Improvements in Undersea Fiber," *CCG Consulting* (blog), September 30, 2021, https://potsandpansbyccg.com/2021/09/30/improvements-in-undersea-fiber/.

[33] The Fiber Optic Association, Inc., "Guide to Fiber Optics and Premises Cabling," https://www.thefoa.org/tech/ref/appln/OSPdatalink.html.

[34] Jose Chesnoy, "Presentation of Submarine Fiber Communication," in *Undersea Fiber Communication Systems*, ed. Jose Chesnoy, 2nd ed. (London: Academic Press, 2016), p. 8.

[35] Juha Saunavaar and Mirva Salmin, "Geography of the Global Submarine Fiber-Optic Cable Network: The Case for Arctic Ocean Solutions," *Geographical Review*, June 2020, pp. 1-9, https://www.tandfonline.com/doi/pdf/10.1080/00167428.2020.1773266.

[36] Telxius, "Telxius Operates the Two Highest Capacity Submarine Cables in the World," press release, December 10, 2018, https://subtelforum.com/telxius-highest-capacity-cables/.

[37] Suresh Kumar, "Celebrating the Completion of the Most Advanced Subsea Cable Across the Atlantic," *Official Microsoft Blog*, September 21, 2017, https://blogs.microsoft.com/blog/2017/09/21/celebrating-completion-advanced-subsea-cable-across-atlantic/.

[38] Deborah Bach, "Microsoft, Facebook and Telxius Complete the Highest-Capacity Subsea Cable to Cross the Atlantic," *Microsoft Features*, September 21, 2017, https://news.microsoft.com/features/microsoft-facebook-telxius-complete-highest-capacity-subsea-cable-cross-atlantic/.

[39] Winston Qiu, "MAREA Cable System Reaches 200 Tbps of Capacity," *Submarine Cable Networks*, October 1, 2018, https://www.submarinenetworks.com/en/systems/trans-atlantic/marea/marea-cable-system-reaches-200-tbps-of-capacity.

In 2021, Google announced that its Dunant undersea cable between Virginia Beach, VA, and Saint-Hilaire-de-Riez, France, was operational, with a carrying capacity of 250 Tbps.[40] Google reached this capacity using "space-division multiplexing" (SDM) technology. SDM increases cable capacity in a cost-effective manner with additional fiber pairs (twelve, rather than the six or eight in traditional subsea cables) and power-optimized repeater designs.[41]

Additionally, recent developments may allow undersea cables to serve multiple functions. The University of Hawaii is a lead institution developing a global network of Science Monitoring And Reliable Telecommunications (SMART) cables that integrate sensors that measure ocean temperature, pressure, and seismicity into commercial undersea telecommunications networks to enhance tsunami and earthquake early warning systems.[42]

Threats to Undersea Telecommunication Cables

Given the heavy reliance on undersea telecommunication cables for consumer, businesses, and government communications, including some military communications, some U.S. officials, industry stakeholders, and scholars have cited the need to protect them from damage. The following section summarizes some of the threats posed to undersea telecommunication cables.

Unintentional Damage to Cables

There are a number of unintentional threats to the physical integrity of undersea telecommunication cables, including commercial fishing and anchoring; natural disasters; and sea life.[43] **Figure 4** presents International Cable Protection Committee (ICPC) data on the causes of cable faults, based on analysis of fault data from 1959 to 2021.

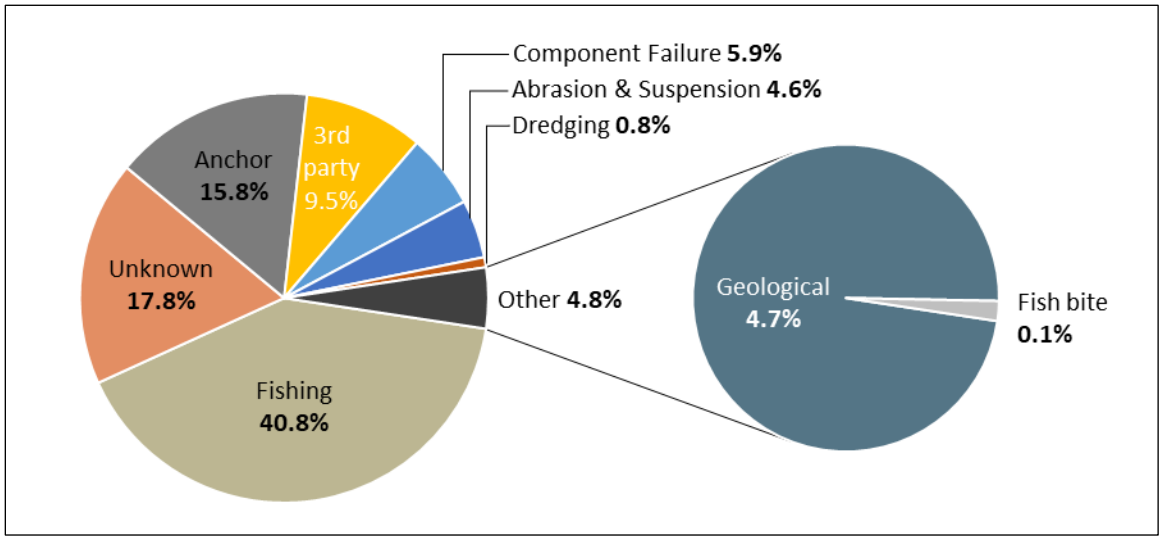
[40] Chris Ciauri, "The Dunant Subsea Cable, Connecting the US and Mainland Europe, Is Ready for Service," Google, February 3, 2021, https://cloud.google.com/blog/products/infrastructure/googles-dunant-subsea-cable-is-now-ready-for-service.

[41] Vijay Vusirikala, "A Quick Hop Across the Pond: Supercharging the Dunant Subsea Cable with SDM Technology," Google, April 5, 2019, https://cloud.google.com/blog/products/infrastructure/a-quick-hop-across-the-pond-supercharging-the-dunant-subsea-cable-with-sdm-technology.

[42] Marcie Grabowski, "Big Boost for Global Network of SMART Seafloor Cables, Early Warning Systems," University of Hawaii at Manoa, School of Ocean and Earth Science and Technology, December 15, 2021, https://www.soest.hawaii.edu/soestwp/ announce/news/big-boost-for-global-network-of-smart-seafloor-cables-early-warning-systems.

[43] Jonathan E. Hillman, *Securing the Subsea Network, A Primer for Policymakers*, Center for Strategic and International Studies, A Report of the CSIS Reconnecting Asia Project, March 2021, https://www.csis.org/analysis/securing-subsea-network-primer-policymakers; see also ODNI Report, pp. 7-8.

Figure 4. Cause of Undersea Telecommunication Cable Faults (1959 to 2021)



Source: Recreated by CRS, from Mike Clare, *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), March 2021, p. 7, https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf.

Notes: The original graphic was generated in 2021, based on analysis of data from a database of reported cable damages kept since 1959. The ICPC report notes that the data was provided courtesy of Global Marine, a British-headquartered company, which provides, installs, maintains, and repairs undersea telecommunications cables.

Human Activities

The ICPC, a non-profit organization formed in 1958 to promote the protection of international undersea telecommunications and power cables, estimates that human activities—fishing, anchoring, and dredging, among others—accounted for roughly two-thirds of undersea cable faults globally between 1959 and 2021.[44] ODNI, in its 2017 report, *Threats to Undersea Cable Communications*, stated that the majority of threats to cables are accidental incidents involving humans.[45] For example, a submarine telecommunication cable was accidentally severed by a ship off the coast of Somalia in 2017, leading to a three-week internet outage costing the country $10 million a day according to a Somali government official.[46]

Natural Disasters

Although undersea telecommunication cables are infrequently damaged by natural disasters (e.g., earthquakes, tsunamis), the impacts of such incidents may be severe and long-lasting. For example, on January 15, 2022, a volcanic eruption and earthquake severed Tonga's only internet connection—an undersea telecommunication cable that connects it to Fiji and other international

[44] International Cable Protection Committee, *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*, Version 1.1, https://www.iscpc.org/publications/icpc-best-practices/.

[45] ODNI Report, p. 6.

[46] "Somalia restores internet connection after weeks of outage," *Reuters*, July 17, 2017, https://www.reuters.com/article/us-somalia-internet-restored/somalia-restores-internet-connection-after-weeks-of-outage-idUSKBN1A21P6; see also Associated Press, "Somalia back online after entire country cut off from internet for three weeks," *The Guardian*, July 17, 2017, https://www.theguardian.com/world/2017/jul/18/somalia-cut-off-from-internet-entire-country-three-weeks.

networks[47]—which took five weeks to fully restore.[48] During the outage mobile network providers offered some connectivity to customers on the main island (where most of the population lives) using satellite connections, although customers reported that capacity was limited, affecting their ability to communicate, connect to the internet, and conduct financial transactions.[49] While repair ships replaced the 56 miles of the international cable connecting Tonga to Fiji (and the rest of the world), the domestic cable, connecting Tonga to its outer islands and the outer islands to each other, is still under repair. In March 2022, Tonga Cable Ltd., Tonga's state-owned cable owner, stated the repairs could take up to a year.[50]

Intentional Damage to Undersea Telecommunication Cables

Some in Congress have expressed concerns over intentional damage to commercial or government-owned undersea telecommunication cables by foreign adversaries and bad actors seeking to disrupt communications or gather personal, corporate, or government information.[51]

In 2017, ODNI reported that while there had been few reported attacks on undersea telecommunication cables, some had been long lasting and impactful. In 2007, Vietnamese pirates stole optical amplifiers, disabling a cable system for 79 days.[52] In 2013, a diver intentionally cut the South East Asia-Middle East-Western-Europe 4 (SMW 4) cable, affecting several service providers, slowing internet speeds by 60% in Egypt.[53] The ODNI report stated that signal rerouting technologies, redundancies in cable lines, and networks of repair ships had increased resiliency of undersea cable networks and reduced the potential that a single cut would cause widespread outages.[54] Further, it asserted that simultaneous attacks against multiple cables could cause "serious long-term disruption,"[55] but are difficult to carry out.

Some North Atlantic Treaty Organization (NATO) defense officials and other foreign affairs analysts have expressed concern that Russia could cut commercial undersea telecommunication cables to disrupt communications.[56] In 2017, U.S. Navy Rear Admiral Andrew Lennon,

---

[47] TeleGeography, "Tonga Cable," https://www.submarinecablemap.com/submarine-cable/tonga-cable.

[48] Associated Press, "Tonga's Internet Is Restored 5 Weeks After Big Volcanic Eruption," *NPR.org*, February 22, 2022, https://www.npr.org/2022/02/22/1082483555/tongas-internet-restored-5-weeks-after-big-eruption.

[49] Chris Duckett, "Digicel Reconnects Tongan Users via Satellite to Rest of the World," *ZDNet*, January 19, 2022, https://www.zdnet.com/home-and-office/networking/digicel-reconnects-tongan-users-via-satellite-to-rest-of-the-world/.

[50] Linny Folau and Mary Lyn Fonua, "Torn Apart, Missing 110km Domestic Fibre Optic Cable May Take Year to Replace," *Matangi Tonga Online*, March 1, 2022, https://matangitonga.to/2022/03/01/torn-apart-missing-fibre-optic-domestic-cable-Tonga.

[51] ODNI Report, p. 22; Morgan Chalfant and Olivia Beavers, "Spotlight Falls on Russian Threat to Undersea Cables," *The Hill*, June 17, 2018, https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables/; see also "Concern over Russian Ships Lurking Around Vital Undersea Cables," CBS News, March 30, 2018, https://www.cbsnews.com/news/russian-ships-undersea-cables-concern-vladimir-putin-yantar-ship/; and David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *New York Times*, October 26, 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

[52] ODNI Report, p. 13.

[53] Ibid.

[54] Ibid, p. 7.

[55] Ibid, p. 8.

[56] 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; Justin Sherman, "Cord-Cutting, Russian Style: Could the Kremlin Sever Global Internet

commander of NATO's submarine forces at the time, reportedly stated, "We are now seeing Russian underwater activity in the vicinity of undersea cables that I don't believe we have ever seen ... Russia is clearly taking an interest in NATO and NATO nations' undersea infrastructure."[57] In 2018, one media outlet, citing a Russian parliamentary publication, reported on Russian capabilities to tap top-secret communication cables, cut undersea cables, and jam underwater sensors.[58] According to an industry expert, "If somebody knew how these systems worked and if they staged an attack in the right way, then they could disrupt the entire system. But the likelihood of that happening is very small."[59]

Repairing Damaged Undersea Telecommunications Cables

Monitoring and repairing commercial undersea telecommunication has generally been the responsibility of the private sector owner/operator(s) of those cables. When a cable is damaged, phone and internet service may be disrupted in certain regions on either end of the cable; service providers often reroute traffic to redundant lines, if available. Cable owners generally test damaged cables from shore by sending a light pulse along the fibers in the cable, which bounces back from the site of the damage.[60] By measuring the time it takes for the light pulse to return, engineers can determine the general area of outage.

Owners rely on commercial cable ships and crews, carrying specialized equipment (e.g., technology to find the exact location of the break, remotely operated submersible vehicles, grappling tools to pull the cable to the surface) to locate, raise, repair, test, and replace the cable to the seabed.[61] In some cases, cable owners' companies agree to carry traffic for each other in event of a cable break, to avoid disruptions in service.[62] In other cases, cable owners employ engineers to conduct or oversee the maintenance and repair of cable that it owns or leases, or contract with a commercial company for repairs; during repairs, it may switch traffic to another route to avoid service disruptions.[63] About 70 cable owners are members of the Atlantic Cable Maintenance and Repair Agreement (ACMA), a non-profit cooperative subsea maintenance

Cables?," *New Atlanticist* (blog), January 31, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/; Sebastian Seibt, "Threat Looms of Russian Attack on Undersea Cables to Shut Down West's Internet," *France 24 News*, March 23, 2022, https://www.france24.com/en/europe/20220323-threat-looms-of-russian-attack-on-undersea-cables-to-shut-down-west-s-internet.

[57] 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.

[58] Deb Reichmann, "Could Enemies Target Undersea Cables That Link the World?," *AP News*, March 30, 2018, https://apnews.com/article/moscow-north-america-ap-top-news-politics-russia-c2e7621bda224e2db2f8c654c9203a09.

[59] 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/.

[60] Lindsay Goldwert, "How Do You Fix an Undersea Cable?," *Slate*, January 8, 2007, https://slate.com/news-and-politics/2007/01/how-do-you-fix-an-undersea-cable.html.

[61] Eric Wagner, "30,000 Feet Below: Connecting Continents from the Ocean Floor," *AT&T Technology Blog*, June 1, 2017, https://about.att.com/innovationblog/undersea_cables.

[62] CSRIC IV, Working Group 8, Submarine Cable Routing and Landing, *Final Report—Protection of Submarine Cables through Spatial Separation* (CSRIC WG8 Spatial Separation Report), December 2014, p. 46, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf.

[63] John Brandon, "Protecting the Submarine Cables That Wire Our World," *Popular Mechanics*, March 15, 2013.

agreement, that offers, among other things, a fleet dedicated to the maintenance of members' cables.[64]

Cyberattacks

Global internet and telecommunications traffic is routed and transported through the undersea telecommunication cable network using advanced information and communication technologies and network management software, making the system vulnerable to cyberattacks. A 2021 think tank report notes that, "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."[65] However, these tools (e.g., software, remote management systems) may create new risks to cable security and resilience.[66] Hackers could access cables through network management systems to skim personal or financial information, hold network management systems hostage until operators pay ransom, or cause widespread disruption in communications.[67]

In April 2022, U.S. Department of Homeland Security Investigations (DHSI) reportedly thwarted a cyberattack on a network of a company that manages an undersea telecommunication cable that provides internet and mobile phone services in Hawaii and in countries across the Pacific region.[68] DHSI officials attributed the attack to an international hacking group, but were not certain of the intent—whether the attacker intended to access business or personal information, hold the system for ransom, or to disrupt communications.[69] DHSI reportedly worked with law enforcement agencies in several countries to make an arrest.[70]

U.S. Actions to Protect Cables

The U.S. government has taken action to protect undersea telecommunication cables. It reviews ownership of cables landing in the United States to identify and mitigate security concerns. It restricts the use of certain vendors and equipment in cables landing in the United States and encourages its allies and partners to do the same. It monitors cables to detect attacks. It invests in cable repair ships to address damage.

[64] ACMA, "FAQs," available at https://www.acma2017.com/about/faqs/.

[65] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council Scowcroft Center for Strategy and Security, September 13, 2021.

[66] Ibid. (The report states that 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." It also notes that hacking a submarine cable may be easier than physically tapping cables, as it can be done remotely.)

[67] Justin Sherman, "The U.S. Should Get Serious About Submarine Cable Security," *Council on Foreign Relations* (blog), September 13, 2021, https://www.cfr.org/blog/us-should-get-serious-about-submarine-cable-security.

[68] CyberTalk, "Hawaii Undersea Cable Attack: A Credential Theft Story," April 22, 2022.

[69] Hawaii News Now, "Federal Agents Disrupted Cyberattack Targeting Phone, Internet Infrastructure on Oahu," April 12, 2022, https://www.hawaiinewsnow.com/2022/04/13/hsi-agents-honolulu-disrupted-cyberattack-undersea-cable-critical-telecommunications/.

[70] Peter Boylan, "Cyberattack on Hawaii Undersea Communications Cable Thwarted by Homeland Security," *Star Advertiser*, April 12, 2022, https://www.staradvertiser.com/2022/04/12/breaking-news/cyberattack-on-hawaii-undersea-communications-cable-thwarted-by-homeland-security/.

Foreign Ownership Review

To operate a cable in the United States, operators must obtain a cable landing license from the FCC. Pursuant to its authorities under the Cable Landing License Act of 1921[71] and Executive Order 10530,[72] the FCC has authority to issue, withhold, or revoke licenses to land or operate commercial undersea telecommunication cables in the United States, provided no such license shall be granted or revoked by the FCC until obtaining approval from the Secretary of State and advice from any executive department the FCC deems necessary.

Additionally, commercial undersea telecommunication cable operators may need to obtain authority to provide international telecommunication services, as required under Section 214 of the Communications Act of 1934, as amended ("the Act").[73] Further, cable operators that co-invest with other entities may need to report foreign ownership interests in undersea cables, if foreign ownership exceeds 10%, as required under Section 310(b) of the act.[74]

When foreign ownership exceeds 10%, the FCC refers the applicant to a group of national security agencies,[75] commonly (and unofficially) known as Team Telecom. Team Telecom reviews applications for national security and foreign affairs concerns, and makes recommendations to the FCC to inform its licensing decisions. On April 4, 2020, President Trump issued Executive Order 13913, which formalized the Team Telecom review process, expanded its membership,[76] and renamed Team Telecom the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector.[77]

In June 2020, DOJ released a statement announcing that Team Telecom recommended the FCC partially deny the Pacific Light Cable Network (PLCN) undersea telecommunication cable system application, due to national security concerns.[78] Team Telecom recommended approval of part of the cable—that which was owned and controlled by Google and Facebook, seeking to connect the United States, Taiwan, and the Philippines. It denied the direct connection between the United States and Hong Kong, due to national security and foreign ownership concerns. In August 2020, Google and Meta (formerly Facebook) revised their cable license, eliminating the connection to Hong Kong.[79] In December 2021, Team Telecom recommended that the FCC grant

[71] 47 U.S. Code Chapter 2.

[72] National Archives, Office of the Federal Register, "Executive Orders" (Executive Order 10530, Part IV), https://www.archives.gov/federal-register/codification/executive-order/10530.html.

[73] 47 U.S.C. §214.

[74] 47 U.S.C. §310(b).

[75] Team Telecom included the Departments of Defense, Homeland Security, and Justice (including the Federal Bureau of Investigation), and consultations with other agencies as needed.

[76] The Committee is chaired by the Attorney General and includes the Secretaries of Defense and Homeland Security; Advisors to the Committee are the Secretaries of Commerce, State, and Treasury; Director of National Intelligence; Administrator of General Services; Director of the Office of Management and Budget; Director of the Office of Science and Technology; U.S. Trade Representative; National Security Adviser; Chair of the Council of Economic Advisers; and Assistant to the President for Economic Policy.

[77] Executive Office of the President, "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," 85 *Federal Register* 19643-19650, April 4, 2020.

[78] DOJ, "Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States," press release, June 17, 2020, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

[79] Todd Shields, "Google, Facebook Dump Plans for U.S.-Hong Kong Undersea Cable," *Bloomberg*, August 28, 2020, https://www.bloomberg.com/news/articles/2020-08-29/google-facebook-dump-hong-kong-cable-after-u-s-security-alarm#xj4y7vzkg.

Google and Meta licenses for their revised cable application.[80] The U.S. government entered into a National Security Agreement with Google and Meta to protect personal data, pursue diversification of interconnection points between the United States and Asia, and restrict access to information and infrastructure by the China-based PLCN partner, Pacific Light Data Communications.[81] In February 2022, the FCC approved the cable landing license for the PLCN connecting the United States to Taiwan and the Philippines.[82]

Restrict Use of Untrusted Equipment

In 2018, the U.S. government identified telecommunication vendors that pose a threat to the national security and foreign policy interest of the United States.[83] In Section 889 of the John S. McCain National Defense and Authorization Act of FY2019 (NDAA, FY2019, P.L. 115-232), Congress named five Chinese equipment-makers as companies "covered" by the restrictions in the law. The law prohibited federal agencies from purchasing equipment or obtaining equipment or systems that use the "covered" equipment; entering into a contract with an entity that uses "covered" equipment; or awarding grants or providing loans for "covered" equipment. The assertion was that the vendors and equipment were untrusted, and if U.S. agencies or grantees installed untrusted equipment in U.S. networks, the Chinese government could potentially capture critical data by compelling vendors to deliver the data to them, or using the equipment to commit espionage against the United States.

Among the vendors named in Section 889 was Huawei Technologies Company (Huawei). Huawei is the world's largest telecommunication network equipment supplier. It makes wireless network equipment (e.g., 4G, 5G), mobile phones, and undersea telecommunication cable equipment, among other things. Its undersea cable segment—Huawei Marine Networks—was among the top five suppliers in the global undersea cable equipment market.[84] By some accounts, it has built or repaired almost a quarter of the world's cables, including upgrades to a cable connecting the United States and Canada, and a cable connecting New York City and London.[85]

In May 2019, the Department of Commerce (DOC) identified Huawei as an entity posing a threat to the national security and foreign policy interests of the United States. DOC cited a Superseding Indictment filed in the Eastern District of New York, alleging that Huawei sold U.S. goods to Iran, violating U.S. sanctions, and engaged in deceptive acts to evade U.S. law.[86] DOC added

[80] DOJ, "Team Telecom Recommends FCC Grant Google and Meta Licenses for Undersea Cable," press release, December 17, 2021, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable.

[81] DOJ, "National Security Agreement," December 13, 2021, https://www.justice.gov/opa/press-release/file/1457291/download.

[82] FCC, "FCC Approves Licenses for PLCN," February 13, 2022, https://www.submarinenetworks.com/en/systems/trans-pacific/plcn/fcc-approves-license-for-plcn.

[83] CRS Report R47012, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests*, by Jill C. Gallagher.

[84] Rebecca Spence, *Industry Report 2021/2022*, Submarine Telecoms Forum, Issue 10, October 25, 2021, p. 50, https://subtelforum.com/products/submarine-telecoms-industry-report/.

[85] Nadia Schadlow and Brayden Helwig, "Protecting Undersea Cables Must Be Made a National Security Priority," *Defense News*, July 1, 2020, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/.

[86] DOJ, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," press release, January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial; and DOC, Bureau of Industry and Security, "Addition of Entities to the Entity List," 84 *Federal Register* 22961-22968, May 21, 2019, https://www.bis.doc.gov/

Huawei to the Bureau of Industry and Security Entity List, which restricts the "export, reexport, and in-country transfer of [U.S.] technology" to listed firms.[87] In response, Huawei sold shares in and segments of its business, including its undersea cable business.[88] The Chinese fiber-optic firm Hengteng Optic Electric purchased Huawei Marine in November 2020, and renamed it HMN Technologies Co., Ltd.[89] Due to the name change, it was able to operate for nearly a year, without restrictions, until the DOC placed HMN Technologies on the Entity List in December 2021.[90]

In 2018, the U.S. Treasury Department designated five Russian entities and several individuals as "covered" for providing material and technological support to Russia's Federal Security Service, known as FSB.[91] Treasury states that since 2007, one of the firms, Divetechnoservices, has procured a variety of underwater equipment and diving systems for Russian government agencies, including the FSB. In 2011, Divetechnoservices was awarded a contract to procure a submersible craft valued at $1.5 million for the FSB. Treasury notes that Russia has been active in tracking undersea communication cables, and Divetechnoservices has contributed to improving Russia's cyber and underwater capabilities, which jeopardize the safety and security of the United States and its allies. For this reason, Treasury added Divetechnoservices and several of its officers to the Entity List for providing material and technological support to the FSB.

In 2022, after Russia invaded Ukraine, the U.S. government took additional action on Russian companies and individuals supporting the FSB. Treasury asserted that an individual set up a front company in Finland to evade U.S. sanctions and procure underwater dive equipment for Divetechnoservices to support the FSB and to improve Russia's cyber and underwater capabilities.[92] Treasury added both the individual and the front company to the Entity List.

Facilitate Investment in Trusted Equipment

Under the Trump Administration, the State Department established the Clean Network Program,[93] which aimed to secure global networks in five areas: U.S. telecommunication networks, mobile application stores, software applications, cloud computing, and undersea cables. The Biden Administration is pursuing similar efforts to build global consensus on network security and encourage the use of trusted equipment and applications and financing alternatives to Chinese-made equipment and undersea telecommunication cables and services. For example, in December 2021, the State Department announced an agreement between Australia, Japan, and the United

index.php/documents/regulations-docs/2394-huawei-and-affiliates-entity-list-rule/file.

[87] DOC, Bureau of Industry and Security, "Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List," 86 *Federal Register* 71557-71568, December 17, 2021.

[88] Huawei Marine Networks is also known as Huawei Marine, HMN Technologies, and HMN Tech.

[89] HMN Tech, "Huawei Marine Networks Rebrands as HMN Technologies," press release, November 3, 2020, https://www.hmntechnologies.com/enPressReleases/37764.jhtml.

[90] DOC, Bureau of Industry and Security, "Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List," 86 *Federal Register* 71559, December 17, 2021.

[91] U.S. Department of the Treasury, "Treasury Sanctions Russian Federal Security Service Enablers," press release, June 11, 2018.https://home.treasury.gov/news/press-releases/sm0410.

[92] U.S. Department of Treasury, "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," press release, March 31, 2022, https://home.treasury.gov/news/press-releases/jy0692.

[93] U.S. Department of State, "The Clean Network (archived content)," https://2017-2021.state.gov/the-clean-network/index.html. The Clean Network was announced by then-Secretary of State Mike Pompeo in August 2020.

States, working in partnership with the Federated States of Micronesia, and with financing from the World Bank and the Asian Development Bank, to build an undersea cable.[94]

On June 26, 2022, President Biden announced a new initiative formed at the 2021 G7 Summit, to launch the Partnership for Global Infrastructure and Investment (PGII).[95] Some see the PGII as a counter to China's Belt and Road Initiative (BRI)—its infrastructure investment program to enhance physical and digital connections between China and the rest of the world, to facilitate trade and economic growth.[96] Similarly, the PGII would mobilize hundreds of billions of dollars for "infrastructure that makes a difference in people's lives around the world, strengthens and diversifies our supply chains, creates new opportunities for American workers and businesses, and advances our national security."[97] Under PGII, a $600 million contract to build an undersea telecommunication cable connecting Singapore to France through Egypt and the Horn of Africa was awarded to U.S. cable company SubCom.[98]

Enhance Cable Security Review

In September 2021, the FCC adopted a set of standardized national security questions that undersea telecommunication cable license applicants with foreign ownership are required to answer and submit directly to the executive branch agencies prior to or at the same time they file their application.[99] The questions address physical and cyber security topics such as network controls access, communications content access, encryption use, and network peering connections.[100] The FCC commissioners agreed that these actions improve the executive branch review process and provide the federal government with needed information for a comprehensive security review.[101] Commissioners Jessica Rosenworcel and Geoffrey Starks urged the FCC to monitor networks beyond the application process to ensure network security and resiliency.[102]

[94] U.S. Department of State, "Joint Statement on Improving East Micronesia Telecommunications Connectivity," press release, December 11, 2021, https://www.state.gov/joint-statement-on-improving-east-micronesia-telecommunications-connectivity/.

[95] The White House, "FACT SHEET: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment," statements and releases, June 26, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment/.

[96] CRS In Focus IF11735, *China's "One Belt, One Road" Initiative: Economic Issues*, by Karen M. Sutter, Andres B. Schwarzenberg, and Michael D. Sutherland. See also "The G7 at last presents an alternative to China's Belt and Road Initiative," *The Economist*, July 7, 2022, https://www.economist.com/china/2022/07/07/the-g7-at-last-presents-an-alternative-to-chinas-belt-and-road-initiative.

[97] The White House, "FACT SHEET: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment," statements and releases, June 26, 2022.

[98] Ibid.

[99] FCC, "Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership." 85 *Federal Register* 7, November 27, 2020.

[100] Ibid, p. 76361 (fn. 4).

[101] See FCC Commissioners statements at FCC, "FCC Improves Transparency and Timeliness of Foreign Ownership Review," October 1, 2020, https://www.fcc.gov/document/fcc-improves-transparency-and-timeliness-foreign-ownership-review.

[102] Ibid.

Monitor Cable Outages

On October 28, 2021, the FCC began requiring submarine cable operators to report specified unplanned service outages or degradation.[103] The FCC collects information through its Network Outage Reporting System to facilitate its "monitoring, analysis, and investigation of the reliability and security of submarine cable networks, and to identify and take action on potential threats to our Nation's telecommunications infrastructure."[104]

Both private owner/operators of undersea telecommunication cables and U.S. agencies actively monitor networks for cyberattacks. The DHSI Cyber Crimes Center works with private sector targets of cyberattacks and international partners, "coordinates investigations of cyber-related criminal activity, and brings together highly technical assets dedicated to conducting trans-border criminal investigations of cyber-related crimes."[105]

Identify Policies and Standards to Protect Cables

The Communications Security, Reliability and Interoperability Council (CSRIC), an FCC advisory committee, whose members include technical experts from the telecommunication industry and federal agencies, published several reports with a series of recommendations to improve undersea cable security. These include the creation of cable protection zones; improved interagency coordination on cable routing; the diversification of routes to increase resiliency and redundancy; the creation of spatial separation requirements or standards to avoid damage from competing marine activities (e.g., installation of power cables and wind farms); and coordination between federal, state, and local agencies and industry (e.g., fishing, shipping) to improve awareness of undersea telecommunication cable vulnerabilities and security needs.[106]

Invest in Cable Repair Vessels

Commercial undersea telecommunication cable owners rely on global private sector companies to lay, maintain, and repair cables. Industry watchers report that with increased demand for undersea cable deployment, installation and repair fleets are booked for several years, which could limit their availability for maintenance and repair of existing cables.[107] While the U.S. government had a ship capable of laying and repairing cable (USNS *Zeus*),[108] some scholars urged the U.S. government to build its repair capacity, and to take more responsibility for repairing cables to

[103] FCC, "Improving Outage Reporting for Submarine Cables and Enhanced Submarine Cable Outage Data," 86 *Federal Register* 22360, April 28, 2021; see also FCC, "Public Safety and Homeland Security Bureau Reminds Submarine Cable Operators of Effective Date of New Outage Reporting Rules," October 28, 2021, https://www.fcc.gov/document/new-submarine-cable-outage-reporting-rules-effective-today.

[104] Ibid, p. 22361.

[105] U.S. Department of Homeland Security, "HSI Cyber Crimes Center," https://www.ice.gov/partnerships-centers/cyber-crimes-center.

[106] For a list of CSRIC reports, see https://www.fcc.gov/CSRICReports.

[107] Rebecca Spence, "Where in the World Are Those Pesky Cable Ships? July 2021," *Submarine Telecoms Forum*, July 23, 2021, https://subtelforum.com/where-in-the-world-are-those-pesky-cable-ships-july-2021/.

[108] Naval Facilities Engineering Systems Command, "Naval Seafloor Cable Protection Office (NSCPO)," https://www.navfac.navy.mil/products_and_services/dc/products_and_services/naval_ocean_facilities_program/sea_floor_cable_protection_nscpo/nscpo_background.html. (The U.S. Navy owns 40,000 miles of undersea cables and maintains a single cable ship—USNS *Zeus*—through the Military Sealift Command, which conducts oceanographic survey and the installation and maintenance of submarine cable systems.)

protect national security.[109] In the NDAA for Fiscal Year 2020 (P.L. 116-92), the U.S. government authorized funding for a Cable Security Program, through which the U.S. government pays for the option to deploy commercial ships in times of emergencies. Through the program, the U.S. government provided $10 million to two privately owned, U.S. flagged ships,[110] each subsidized at $5 million per year, to continuously operate the vessels in the commercial submarine cable services market (including the laying, maintenance, and repair of submarine cables) and provide the U.S. government access to the vessels in times of national emergency.[111] The intent of the program is to meet national security requirements and to maintain a U.S. presence in the international submarine cable services market.[112]

Issues for Congress

Given the importance of commercial undersea telecommunication cables to consumer, business, and government communications, Congress may consider several policy options to address risks to the commercial undersea telecommunication cable network.

Role of U.S. Government in Protection of Cables

Congress may consider the role of the U.S. government in securing commercial undersea telecommunication cables. The DHS Communications Sector Specific Plan, issued in 2015 by DHS, emphasizes the need to work with the private sector to ensure the security and resiliency of communication systems. The Plan focuses on fiber networks serving communities and businesses with broadband services, but does not mention undersea telecommunication cables specifically.[113] Congress could direct DHS to update its Communications Sector Specific Plan and related Information Technology Sector-Specific Plan, and include specific recommendations for enhancing security and resiliency of undersea cables. Congress could establish a formal framework to ensure security of cables, similar to that used for pipelines, under the Transportation Security Administration within DHS.[114]

Congress may consider the recommendations of the CSRIC to appoint a lead agency to coordinate undersea telecommunication cable security, or establish an interagency working group

[109] Nadia Schadlow and Brayden Helwig, "Protecting Undersea Cables Must Be Made a National Security Priority," *Defense News*, July 1, 2020, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/. See also Bert Chapman, *Undersea Cables: The Ultimate Geopolitical Chokepoint*, Purdue University, FORCES Initiative: Strategy, Security, and Social Systems, December 13, 2021, p. 9, https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1000&context=forces. Citing an unintentional cut in three undersea cables connecting Italy and Egypt, disrupting 80% of the connectivity between Europe and the Middle East, the author states this was "particularly problematic for the U.S. and British militaries, which had 200,000 troops in Iraq at that time and relied on commercial undersea cable networks for 95% of their strategic communications," demonstrating the national security concern.

[110] U.S.-flagged vessel means any vessel registered under the laws of the United States (26 U.S.C. §1355).

[111] Department of Transportation, Maritime Administration, "Request for Application to be Considered for Enrollment in the Cable Security Fleet," 86 *Federal Register* 355, January 5, 2021.

[112] For more information, see CRS Report R46654, *U.S. Maritime Administration (MARAD) Shipping and Shipbuilding Support Programs*, by Ben Goldman. See also "*C.S. Decisive* reflagged for U.S. Cable Security Fleet," *American Maritime Officer* (Vol. 52, No. 2), February 2022, https://www.amo-union.org/news/2022/202202/202202.pdf. (Noting that SubCom's cable ship, *C.S. Dependable* was reflagged into U.S. registry in December 2021 and SubCom's cable ship, *Decisive*, was reflagged into U.S. registry in January 2022 for service in the two-ship U.S. Cable Security Fleet.)

[113] DHS, *Communications Sector-Specific Plan: An Annex to the NIPP 2013*, 2015, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf.

[114] For further details, see CRS Report R46903, *Pipeline Cybersecurity: Federal Programs*, by Paul W. Parfomak and Chris Jaikaran.

to coordinate cable security to increase its oversight of cables and cable technologies. It could extend FCC's authorities to ensure security of new and existing cables, coordinate federal agency review of cable applications, and disseminate undersea cable security information to other federal agencies. Congress could also consider a recommendation contained in the 2017 ODNI report to delegate authority to an agency to build public-private partnerships to secure cables, to set standards for security, and promote those standards globally. Alternatively, it may conclude that no further action is needed and continue to rely on the private sector and private agreements for protection of commercial cables.

Another approach could be to increase the number of landing stations in the United States to attract new cables and to increase the resiliency and redundancy of the U.S. telecommunication network. Some Members have proposed legislation to incentivize states to build cable landing stations, as in S. 1166, introduced in the 116th Congress. The Infrastructure Investment and Jobs Act (P.L. 117-58) includes undersea telecommunications cables and landing stations as an allowable expense under Middle Mile Grant Program, funded under the act.

Connections with Adversarial Nations

Congress may consider whether the U.S. government should restrict U.S. firms from constructing undersea telecommunication cables that connect the United States to the territory of adversarial nations or from entering into partnerships with companies from those countries. Congress could continue to rely on the existing process whereby the FCC refers applications to Team Telecom for review, where Team Telecom reviews undersea cable license applications and identifies national security concerns for the FCC, and the FCC considers Team Telecom recommendations in its decision to approve, deny, modify, or condition any license application. Some Members have proposed legislation, such as in H.R. 4029 (117th Congress), to codify the Team Telecom national security review process and to increase interagency coordination.

Some security experts assert that landing a cable in an adversarial nation may increase an adversary's ability to tap or intercept sensitive commercial and private information and should be restricted. However, restricting connections to specific countries could affect economic gains for U.S. companies. For example, in the Asia-Pacific region, submarine cables have typically landed in one of a few hubs, including Japan, Singapore, and Hong Kong. Since cables commonly land in these hubs, data centers are also concentrated there. Limiting the ability of U.S. companies to land cables in Hong Kong, or to access data centers in Hong Kong, could limit their ability to serve the Hong Kong market or beyond. Limiting connections between the United States and China may force Chinese companies to connect cables to countries other than the United States and to move their data centers or spur new data centers near those cable landing stations.

A 2020 report published by Johns Hopkins Applied Physical Laboratory asserts that restricting the participation of U.S. firms in undersea cable projects that connect the United States to a Chinese territory could reduce "the availability and resilience of network connectivity between the United States and the Asia Pacific [region]" and that "global data storage and processing capacities would potentially migrate out of the United States."[115] Congress may consider how to best mitigate national security concerns associated with commercial undersea cable projects that land in the territories of nations deemed to be adversarial to the interests of the United States, while addressing potential economic impacts of those mitigation measures.

[115] Paul Triolo, *The Telecommunications Industry in U.S.-China Context: Evolving Toward Near-Complete Bifurcation*, The Johns Hopkins Applied Physics Laboratory, 2020, pp. 16-17, https://apps.dtic.mil/sti/pdfs/AD1116899.pdf.

Restrictions on Technologies or Technology Firms

Congress may consider additional restrictions on any cable terminating in U.S. territory from containing equipment from adversarial nations. While additional restrictions may curb the use of this equipment in new cables, they do not address the presence of untrusted equipment in existing undersea cable networks. Thus, Congress may also consider increased support for monitoring existing cables terminating in U.S. territory and investing in the development of new technologies for monitoring or defending against a cyberattack on existing undersea telecommunication cables.

Strengthening Security Requirements

Congress could strengthen or direct the FCC to strengthen security requirements for commercial undersea telecommunication cables landing in the United States beyond restrictions on certain foreign equipment, such as establishing spatial requirements and requirements to avoid clustering of cables, creating cable protection zones, diversifying routes, and installing redundant cable lines—as the CSRIC has recommended.[116]

Congress could also direct agencies such as the FCC, DHS, DOD, and Department of State or advisory bodies to work with industry to develop standards and criteria for improving commercial undersea telecommunication cable security, voluntarily or through mandates. Congress may encourage agencies and U.S. entities to engage in international organizations, such as ICPC. Further, Congress may encourage or incentivize participation in the International Telecommunications Union, an agency of the United Nations focused on improving global communications, to promote U.S. recommendations for improving undersea telecommunication cable security.

Addressing the Risk of Damage Through Commercial Activity

Congress may choose to address accidental damage by fishing vessels—a major cause of undersea telecommunication cable faults. Congress could direct DHS to facilitate coordination between industries (e.g., telecommunication, energy, fishing) and develop recommendations or best practices to improve security and resiliency of undersea cables. Congress could direct the FCC to seek public comment on CSRIC recommendations and adopt rules to strengthen the security and resiliency of cables. Congress could direct the FCC or DHS to identify cables at the highest risk of damage (e.g., in high traffic areas, clustered at certain landing points, single points of failure) and develop damage mitigation polices and measures for those cables. Congress could also impose steeper fines for damages.

Conclusion

Because the global commercial undersea telecommunication cable network carries about 95% of intercontinental global internet traffic and 99% of transoceanic digital communications, it is

[116] These recommendations apply to cables within U.S. jurisdiction. Commercial cables that extend from the United States beyond U.S. territorial waters are not fully under the jurisdiction of the U.S. government. For cables that extend beyond U.S. territorial waters, several international treaties dating from 1884 define the treatment of cables, establish a state's rights to lay cables in international waters, maintain cables, and impose punishment for damage to cables. While the United States has not ratified the latest treaty governing cables, the United Nations Convention on the Law of the Sea (UNCLOS), it has codified the terms of the treaty as they relate to undersea cables (47 U.S.C. Chapter 2). For a discussion of the treaties governing international undersea telecommunication cables, see CSRIC, *WG8 Spatial Separation Report*, December 2014, pp. 42-46.

essential infrastructure for information exchange and commerce. In addition to natural threats to this infrastructure, there are inadvertent threats from human activity such as commercial fishing and shipping as well as deliberate damage and disruption of service by a variety of threat actors. Congress may examine the U.S. approach to commercial undersea telecommunication cable security and consider policies to strengthen it. It may conclude that commercial undersea telecommunication cable security should remain primarily the responsibility of private sector cable owners and consider policies that incentivize cable owners to increase their security posture. Alternatively, Congress may determine that, due to the centrality of the global commercial undersea telecommunication cable network to information exchange and commerce, it should consider policies that strengthen coordination and cooperation among federal agencies and with the private sector to ensure security of the cable network.

Author Information

Jill C. Gallagher
Analyst in Telecommunications Policy

Disclaimer