# The Global Submarine Cable Network, Cybersecurity and Resilience, and Risks to U.S. National Security

Written Testimony

Justin Sherman
Founder and CEO, Global Cyber Strategies
Nonresident Senior Fellow, Atlantic Council's Cyber Statecraft Initiative

U.S. Senate Committee on Commerce, Science, and Transportation

Subcommittee on Communications, Media, and Broadband

Hearing on "Communications Networks Safety and Security"

December 11, 2024

---

Subcommittee Chair Luján, Ranking Member Thune, and distinguished members of the Subcommittee, I appreciate the opportunity to testify today about the global submarine cable network, cybersecurity and resilience, and protecting our national security from foreign threats.

I am the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm, and a nonresident senior fellow at the Atlantic Council's Cyber Statecraft Initiative. I teach, consult, research, and write on cybersecurity, privacy, submarine cable resilience, geopolitical risk, and China and Russia—and am sanctioned by the Russian government. I'm also the author of the forthcoming book *Technology and National Security Collide*, on the history and future of US national security regulations and review programs focused on technology.

Hundreds of submarine cables globally carry 99% of internet traffic between continents. This network's security and resilience are vital to worldwide information flows, commerce, scientific research, military communications, and US national security. Private-sector companies' ability to competitively build and maintain this network is also vital: to economic security, national security, and the US' ability to differentiate its internet approach from Beijing's model. Simultaneously, companies involved in subsea cables often have major national security blind spots, and foreign actors, particularly the Chinese and Russian governments, pose sophisticated, persistent threats to the global submarine cable network and the security of US data flows. This makes the interagency "Team Telecom" committee critical to protecting US national security, countering Chinese state efforts to compromise the cable supply chain, and helping companies to better understand the risks.

Congress should keep encouraging Team Telecom's transparency; statutorily authorize Team Telecom to ensure it has appropriate authorities and funds; commission a study on Beijing's threats to submarine cables; and request a Team Telecom lessons-learned report to inform future action.

In this written testimony, I describe how:

- Submarine cables globally carry 99% of internet traffic between continents. There are more than 500 submarine cables "in service" worldwide, with dozens more underway.
- Private-sector American companies have long played a pivotal role in the financing, construction, laying, and management of submarine cables connected to the United States and between other countries around the world. Historically, cable investment and ownership from the United States was led by firms such as AT&T and Verizon. Today, the dominant US investors in and owners of submarine cables are Alphabet (Google), Amazon, Meta (Facebook), and Microsoft. They are pouring money into these activities.
- Worldwide, a variety of entities—private-sector, government, and both—are involved in financing, constructing, laying, and managing submarine cables. Not every country has what are typically considered large internet companies driving subsea cable investments.
- Submarine cable projects are highly expensive, resource intensive, and logistically complex—and frequently cross many borders. International collaboration on financing, constructing, laying, managing, and repairing submarine cables is therefore an important, necessary, and largely positive fact of maintaining and expanding the global network.
- There are many threats to submarine cables: accidents, natural weather events, and persistent, ongoing risks of espionage, sabotage, disruption, and supply chain infiltration from foreign actors, particularly from the Chinese and Russian governments. These threats put at risk the cable network, its cybersecurity and resilience, and US national security.
- More than 80% of the hundreds of cable outages and breaks each year are due to fishing and anchoring incidents, and many of the remainder are due to natural weather events. However, industry does not always capture or appreciate the national security risks at play.
- Submarine cables are a potential surveillance goldmine. Foreign actors can potentially tap into cables at multiple points throughout the route, including by hacking into cable-adjacent, internet-connected systems. Malicious actors can also physically damage cables, and while cutting one cable is not going to knock out the world's internet, damaging or destroying cables in certain regions can disrupt some data flows, have the effect of encouraging traffic to flow via other means, force repair ships to be sent out, and more.
- Recent cable cuts in the Baltic Sea by a Russia-departing Chinese vessel, an attempted cyber operation against a cable-linked system in Hawaii, accidental cable cuts in the Red Sea due to the Houthis sinking a ship, and suspicious Chinese government and company activity near Asia-Pacific cables, among others, speak to these security risks.
- Chinese state-owned telecoms China Mobile, China Telecom, and China Unicom are also major Chinese investors in subsea cables, and Russia's Main Directorate for Deep Sea Research is accelerating development of undersea surveillance and targeting capabilities.
- For decades, an informal interagency group, dubbed "Team Telecom," advised the Federal Communications Commission on the national security risks to infrastructure like submarine cables. President Trump formally established Team Telecom as an executive branch committee with E.O. 13913 in 2020, which President Biden kept in place. Today, Team Telecom plays a vital role in advising the FCC on the national security risks to cables.
- Recent Team Telecom decisions informed the FCC's effective expulsion of China Telecom from the United States in 2021 and mitigations for a proposed cable that would have had landing stations in California and in Hong Kong. Team Telecom's bipartisan-supported work must continue—and is even more essential given threats from Beijing and Moscow.

**The Global Submarine Cable Network**

Submarine cables globally carry 99% of internet traffic between continents.[1] These cables vary in thickness from about one centimeter to about 20 centimeters, about the thickness of a garden hose, and contain a hair-thin inner fiber than transmits internet data across the cable, whether emails, videos, or sensitive documents.[2] Fiber-optic cables are faster, cheaper, and generally more reliable than satellites.[3] (In fact, while satellite communications have important uses and value-adds in specific, defined scenarios, it's on the whole not even close in speed, bandwidth, and reliability, among other metrics.)[4] Companies and other entities build different components of these cables, assemble them, and lay them across the ocean floor to connect disparate masses, like South America and Europe. Every undersea cable has at least two "landing points," or the locations where the cable meets the shoreline. Facilities at these landing points can provide multiple functions, including terminating an international cable, supplying power to the cable, and acting as a point of domestic and/or international connection.[5] The owner of a submarine cable may not be the same entity as the owner of the landing station, just as a company or government agency that invests in a submarine cable's construction may not be the same entity managing its operation once live.

As of September 2024, according to TeleGeography, there are 532 cable systems "in service" (actively operating) around the world—with another 77 cable systems planned and on the way.[6] This number is continually growing, due to companies' investments, and for some countries, governments' investments, in the infrastructure; increased digital connectivity; growing consumer and business use of online services with greater data demands; and new data center demands driven by the explosion of cloud service provider infrastructure and the explosion of companies and other organizations training and deploying artificial intelligence (AI) and machine learning (ML) applications, among others.[7] Even systems like 5G telecommunications networks will likely

[1] This figure was broken down well by Alan Mauldin for TeleGeography: Alan Mauldin, "Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?" TeleGeography.com, May 4, 2023, https://blog.telegeography.com/2023-mythbusting-part-3.

[2] This and other portions of this testimony point to: Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security* (Washington, D.C.: Atlantic Council, September 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/, 4. As noted in the report, on the page cited, thanks as well to experts such as Bill Woodcock for discussion of these points at the time of the 2021 report's authoring.

[3] For some good explainers, see, e.g., Jeff Fraleigh, "Fiber vs. Satellite Internet: Why Fiber Optics Lead the Future of High-Speed Connectivity), ETI Software, April 24, 2024, https://etisoftware.com/resources/blog/fiber-vs-satellite-why-fiber-optics-lead-the-future-of-high-speed-connectivity/; Airband, "Fibre optic vs. satellite: What's the difference?" Airband.co.uk, accessed December 3, 2024, https://www.airband.co.uk/fibre-optic-vs-satellite-difference/.

[4] Of course, other nuances exist too, such as how these means of communications transmission can interact.

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

[6] Lane Burdette, "How Many Submarine Cables Are There, Anyway?" TeleGeography.com, September 9, 2024, https://blog.telegeography.com/how-many-submarine-cables-are-there-anyway.

[7] See, e.g., Ibid.; Emma Chervek, "Ciena CTO talks subsea cables, data center efficiency vs. demand," SDXCentral.com, November 2, 2023, https://www.sdxcentral.com/articles/interview/ciena-cto-talks-subsea-cables-data-center-efficiency-vs-demand/2023/11/; Diana Goovaerts, "Thanks to cloud, hyperscalers are changing the way subsea cables make landfall," Fierce-Network.com, September 26, 2023, https://www.fierce-network.com/data-center/hyperscalers-are-changing-way-subsea-cables-make-landfall.

increase submarine cable demands in some form or another, as the mobile telecom networks send more and more data to, and retrieve more and more data from, internet data servers and cloud infrastructure located around the world. All to say, submarine cables are critical to global communication flows—and the modern internet as we know it would not exist without this subsea cable network.

Private-sector American companies have long played a pivotal role in the financing, construction, laying, and management of submarine cables connected to the United States and between other countries around the world.[8] Historically, cable investment and ownership from the United States was led by firms such as AT&T and Verizon. Today, the dominant US investors in and owners of submarine cables are Alphabet (Google), Amazon, Meta (Facebook), and Microsoft.[9] These four companies have invested in and bought major capacity on dozens of subsea cables around the world in recent years,[10] making clear that they do not just have outsized influence in areas such as cloud computing, social media, e-commerce, and search but physical internet infrastructure under the ocean. Alphabet, Amazon, Meta, and Microsoft's investment ramp-up has been tremendous. In roughly a decade, the content providers (such as Meta and Alphabet) went from consuming 6.3% of total international cable capacity to 69% of total international cable capacity, and these four companies went from investing in only one long-distance subsea cable to investing in dozens and dozens.[11]

Looking forward, these four companies are going to spend even more money on subsea cables and increase their influence over the global infrastructure even further in the next decade. Just several days before this hearing, for instance, *TechCrunch* reported that Meta is planning to build a new subsea cable more than 40,000 kilometers (~24,855 miles) long that could require more than $10 billion in investment—with Meta to be the cable's sole owner and user.[12]

Worldwide, a variety of entities are involved in financing, constructing, laying, and managing submarine cables. As of September 2021, for example, 65% of submarine cables had a single owner and 33% had multiple owners (and 2% without readily accessible ownership data).[13] Approximately 59% of cables had only private owners, 19% had all state owners, and 19% had both private and state owners (and 3% without readily accessible data).[14] The organizations involved in different elements of the submarine cable supply chain, including financing, are wide-ranging: from content providers such as Google; to large, traditional telecommunications companies like Vodafone, Airtel, and Algar Telecom; to investment firms like SoftBank; to subsea

---

[8] For an excellent discussion and analysis of some of this history, see: Nicole Starosielski, *The Undersea Network* (Durham: Duke University Press, 2015).
[9] See, e.g., Global Data, "Hyperscalers turning the tide in subsea cables," *Yahoo! Finance*, December 6, 2024, https://finance.yahoo.com/news/hyperscalers-turning-tide-subsea-cables-150705832.html.
[10] Alan Mauldin, "A (Refreshed) List of Content Providers' Submarine Cable Holdings," TeleGeography.com, June 27, 2024, https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new.
[11] Andrew Blum and Carey Baraka, "Sea change," Rest of World, May 10, 2022, https://restofworld.org/2022/google-meta-underwater-cables/, citing TeleGeography data; Global Data, "Hyperscalers turning the tide in subsea cables."
[12] Ingrid Lunden, "Meta plans to build a $10B subsea cable spanning the world, sources say," *TechCrunch*, November 29, 2024, https://techcrunch.com/2024/11/29/meta-plans-to-build-a-10b-subsea-cable-spanning-the-world-sources-say/.
[13] Sherman, *Cyber Defense Across the Ocean Floor*, 7.
[14] Ibid., 9.

cable manufacturers like SubCom, Alcatel, and Huawei Marine; to state-owned entities such as Djibouti Telecom, Instituto Costarricense de Electricidad, and the Telecommunication Infrastructure Company of Iran; and many more. Not every country has what are typically considered large internet and platform companies driving submarine cable investments.

Submarine cable projects are highly expensive, resource intensive, and logistically complex. It is worth reemphasizing that it has been and will likely remain a largely positive—and necessary—fact that so many different organizations around the world are able to collaborate on continuing to build out the global submarine cable network to meet resiliency challenges and deliver speed, bandwidth, and so on. Likewise, the US private sector has played a significant role in helping to build out the global subsea cable network, and it is essential for them to be able to continue doing so. At the same time, however, there are considerable risks to submarine cables—and, related, to national security—that demand policymaking and other involvement from the US government.

**Risks to Submarine Cables**

There are many threats and risks to the global submarine cable network. These threats span accidents (responsible for most damage to subsea cables each year), natural weather events, and persistent, ongoing risks of espionage, sabotage, disruption, and supply chain infiltration from foreign actors, particularly from the Chinese and Russian governments. Such threats, particularly from Beijing and Moscow, put at risk not just the global cable network and its cybersecurity and resilience—but US national security.

Most of the publicly documented instances of damage and disruption to submarine cables around the world are due to accidents, such as boats moving close to a shoreline, not properly checking their maps for cables in the area, and then accidentally ripping up or damaging a cable with a dragging anchor. Other incidents of damage and disruption, though far less frequent than accidents, are caused by natural weather events, such as underwater earthquakes, underwater volcanic eruptions, and abrasion and erosion that damage cables and require repairs.[15] In May 2024, for example, the International Cable Protection Committee said that more than 80% of all cable outages and breaks are due to fishing and anchoring incidents.[16] There are typically hundreds of incidents of damage to submarine cables reported every year (lately, around 150-200 annually),[17] and most of those incidents—as with the vast majority of all damage to subsea cables since 1959—fall into the category of accidents caused in shallow water.[18] It is important to recognize this data for at least two reasons: companies and governments need to keep ensuring robust, rapid repairs to maintain the global subsea cable network's resilience; and the US government needs to ensure

[15] Mike Clare, *Submarine Cable Protection and the Environment* (Portsmouth: International Cable Protection Committee, March 2021), https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf, 4-5.
[16] Graham Evans, "Report of the International Cable Protection Committee," Presentation for International Hydrographic Organization: Hydrographic Services and Standards Committee, May 27-31, 2024, https://iho.int/uploads/user/Services%20and%20Standards/HSSC/HSSC16/HSSC16_2024_07.10A_EN_ICPC%20activities%20affecting%20HSSC.pdf, 5.
[17] International Telecommunication Union, "Launch of international advisory body to support resilience of submarine telecom cables," ITU.int, November 29, 2024, https://www.itu.int/en/mediacentre/Pages/PR-2024-11-29-advisory-body-submarine-cable-resilience.aspx.
[18] Clare, *Submarine Cable Protection and the Environment*, 4-5.

its understanding of the cable landscape incorporates this data and does not get distracted by occasional media stories on scenarios such as sharks attacking subsea cables.[19]

There are also routine risks to submarine cables that result from criminals and other malicious actors looking to exploit vulnerabilities in technological systems and take advantage of companies with insufficient investments in basic cybersecurity best-practices, such as comprehensive multifactor authentication, robust encryption, access controls, audits, continuous monitoring, supply chain security assessments, vendor and contractor controls, meaningful empowerment and resourcing of company decision-makers and staff focused on cybersecurity, and so on.

At the same time, however, the data on ships accidentally dragging their anchors and telecoms getting hacked by criminals does not adequately capture another important risk set: risks from sophisticated foreign threat actors, particularly the Chinese and Russian governments.

*Espionage:* Submarine cables are a potential surveillance goldmine. For well over a century, nations have used their access to cables to conduct espionage, such as when British intelligence, in the late nineteenth century, used an international hub of telegram cables in Porthcurno to gain eavesdropping advantage.[20] Today's submarine cables carry enormous volumes of data—as mentioned, 99% of all intercontinental internet traffic in the world. Foreign actors can potentially tap into these cables at multiple points throughout the cable route (e.g., as the cable is exposed above water when coming up on the shoreline, at landing stations, by putting a cable landing point in a place under state control) and in the cable supply chain (e.g., during installation, repairs), including by hacking into the remote, internet-connected software systems (and the other systems around them) that companies increasingly use to manage submarine cable networks.[21] These latter systems can increase the cybersecurity attack surface for cable networks. The many actors involved in cable financing, construction, laying, management, and repair also create opportunities for governments and government-linked actors to exert influence over submarine cables and the broader submarine cable network, such as by legally requiring or extralegally coercing companies or individuals at those companies to assist with government surveillance operations.

*Damage and Disruption:* Malicious actors could also damage cables with the intent of disrupting traffic flows or blacking out subsea cable traffic to an area. To be clear, in most cases, chopping a subsea cable is not going to sever an entire country's internet. (There are some narrow cases where this is possible, such as when a devastating volcanic eruption in 2022 off the coast of Tonga

[19] See, e.g., Peter H. Lewis, "Phone Company Finds Sharks Cutting In," *The New York Times*, June 11, 1987, Section A, Page 1; Tim Starks, "Sharks, earthquakes and cyberattacks: The threats to undersea cables," *The Washington Post*, June 28, 2023, https://www.washingtonpost.com/politics/2023/06/28/sharks-earthquakes-cyberattacks-threats-undersea-cables/. See also: "Sharks are not the Nemesis of the Internet—ICPC Findings," International Cable Protection Committee, July 1, 2015.

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

[21] See, e.g., DJ Pangburn, "Wiretapping Undersea Fiber Optics Is Easy: It's Just a Matter of Money," *VICE*, July 22, 2013, https://www.vice.com/en/article/undersea-cable-surveillance-is-easy-its-just-a-matter-of-money/; Jonathan E. Hillman, *Securing the Subsea Network: A Primer for Policymakers* (Washington, D.C.: Center for Strategic & International Studies, March 2021), https://www.csis.org/analysis/securing-subsea-network-primer-policymakers, 10; Sherman, *Cyber Defense Across the Ocean Floor*, 17.

damaged a submarine cable and knocked out the country's internet connectivity.)[22] Nor is one cable cut going to bring down the global internet and knock the world's communications offline. But damaging or destroying cables in certain regions can disrupt some data flows, have the effect of encouraging traffic to flow via other means (e.g., through a new point from which traffic can be intercepted), force repair ships to be sent out, and much more. There is much discussion in the submarine cable space, and especially among academics and industry experts working at the United Nations and other bodies, of norms—including norms of what governments will and will not do to submarine cables. While these are important discussions, including insofar as they encourage dialogue between countries, it is impractical to think that in a wartime, armed conflict, or crisis scenario, a country with sophisticated military and intelligence capabilities would not be willing to violate what some consider a norm and attack submarine cable infrastructure. (Of course, some would hold this norm does not even exist now.) This is especially the case when considering the normative postures of governments in Beijing and Moscow.

*Strategic Network-Shaping:* At a higher level, cable construction and maintenance can provide strategic value to governments. Many private-sector and government actors, frequently in collaboration, are involved in important submarine cable construction activities. Building more cables in and of itself, in a sense, arguably increases the resilience of the global internet in absolutist terms: there are new routes over which data can travel in the event of failure. But choosing where, when, and how to build cables is also a way to shape where global internet traffic is routed.[23] Changes to traffic routing patterns generate profits for companies and can move new volumes of traffic through different countries' borders—which can enable data interception and the development of technological dependence.[24] This is an important consideration as authoritarian governments increasingly work to reshape the internet's physical topology (structure) and digital behavior by exerting control over companies.

For example, among other events that underscore national security risks to submarine cables:

- Cable Cuts in Baltic Sea: In November 2024, a Chinese bulk carrier, the Yi Peng 3, dragged its anchor along the Baltic Sea's seabed for over 100 miles and severed two undersea cables: one between Sweden and Lithuania and another between Finland and Germany.[25] When the ship traveled through the Baltic Sea, it also crossed over four gas and oil pipelines, a power line, and another subsea cable under construction.[26] As others have already noted, it is extremely unlikely a ship would accidentally have an anchor drag for

[22] Ian Ralby and Justin Sherman, "Tonga's Devastating Volcanic Eruption Has Left the Island Without Internet," *Slate*, January 21, 2022, https://slate.com/technology/2022/01/tonga-volcano-internet-underseas-cables.html.
[23] This is reflected in the fact that "traffic that appears to be traveling via separate network paths could potentially be relying on the same physical resource." Zachary S. Bischof, Romain Fontugne, and Fabián E. Bustamante, "Untangling the world-wide mesh of undersea cables," *HotNets '18: Proceedings of the 17th ACM Workshop on Hot Topics in Networks* (November 2018): 78-84, https://dl.acm.org/doi/abs/10.1145/3286062.3286074, 81.
[24] Sherman, *Cyber Defense Across the Ocean Floor*, 10.
[25] Bojan Pancevski, "Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables," *The Wall Street Journal*, November 29, 2024, https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1; Bojan Pancevski, "Russia Suspected as Baltic Undersea Cables Cut in Apparent Sabotage," *The Wall Street Journal*, November 20, 2024, https://www.wsj.com/world/europe/russia-suspected-as-baltic-undersea-cables-cut-in-apparent-sabotage-801cb392.
[26] Sophie Tanno, "Sweden asks China to cooperate in Baltic Sea cable investigation," CNN, November 29, 2024, https://www.cnn.com/2024/11/29/europe/sweden-china-baltic-sea-cable-intl/index.html.

100 miles without immediately noticing the impacts on speed. Germany's defense minister has said the damage appears to be sabotage, but did not yet specify any further evidence.[27] Investigations are reportedly still unfolding in Europe, and complicating the situation further is that the ship originally departed from Vistino, Russia.[28] (As Lithuania's Foreign Minister commented, this incident, to him suspiciously, follows a Chinese-registered vessel damaging two subsea cables in the Baltic Sea in October 2023.)[29]

- Attempted Cyber Attack or Intrusion in Hawaii: In 2022, agents at the Department of Homeland Security's Homeland Security Investigations arm said they disrupted what they described as a cyber attack on a critical undersea cable linking Hawaii and the Pacific.[30] DHS said "an international hacking group" had carried out a "significant breach involving a private company's servers associated with an undersea cable" and that "HSI agents and international law enforcement partners in several countries were able to make an arrest"[31]—suggesting a threat actor or actors based outside of the United States.
- Damages in South China Sea: Cables around Taiwan have been cut over two dozen times in the last five years, typically due to Chinese vessels, or vessels that are suspected to be from China, severing the cables.[32] Chinese sand dredgers have reportedly accounted for at least 10 of these breaks.[33] Some experts, in response, have noted both the frequency of accidental submarine cable damage around the world—and others the strangeness of many similar, repeat incidents in a highly monitored and contested zone of the world.
- Chinese Coast Guard near Vietnam: The *Washington Post* reported in October 2024 that, in April 2024, a Vietnamese naval vessel was escorting a crew aboard a private subsea cable ship within Vietnam's 200-mile exclusive economic zone, when a Chinese coast guard vessel confronted the ships. (As noted in the story, this is hundreds of miles from the Chinese mainland.) Then, "the Chinese vessel came within one mile of the repair ship and demanded over radio to know the nature of the ship's activities, according to executives at the cable company as well as photos of the encounter between the two vessels and text messages from the repair crew on the day of the incident… After the Vietnamese naval ship withdrew several miles away, the Chinese ship spent a day circling the repair vessel,

[27] Shweta Sharma, "Sweden formally asks China to cooperate with investigations into undersea cables damage," *The Independent*, November 30, 2024, https://www.the-independent.com/asia/china/sweden-china-cable-damage-baltic-sea-b2656390.html.
[28] Tanno, "Sweden asks China to cooperate in Baltic Sea cable investigation."
[29] Sophia Besch and Erik Brown, "A Chinese-Fallged Ship Cut Baltic Sea Internet Cables. This Time, Europe Was More Prepared," Carnegie Endowment for International Peace, December 3, 2024, https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en.
[30] "Federal agents disrupted cyberattack targeting phone, internet infrastructure on Oahu," Hawaii News Now, April 12, 2022, https://www.hawaiinewsnow.com/2022/04/13/hsi-agents-honolulu-disrupted-cyberattack-undersea-cable-critical-telecommunications/.
[31] AJ Vicens, "DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii," *CyberScoop*, April 13, 2022, https://cyberscoop.com/undersea-cable-operator-hacked-hawaii/.
[32] Huizhong Wu and Johnson Lai, "Taiwan suspects Chinese ships cut islands' internet cables," Associated Press, April 18, 2023, https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70.
[33] Rachel Cheung, 'A Warning Sign': Chinese Ships Accused of Cutting Off Internet to a Taiwanese Island," *VICE*, March 17, 2023, https://www.vice.com/en/article/taiwan-internet-cables-matsu-china/.

then left it, and the crew finished the job." The company's head of maintenance said it was clearly a "show of strength" by the Chinese coast guard ship.[34]

- Russia's GUGI: US officials told CNN in October 2024 that Russia is building up its fleet of surface ships, submarines, and naval drones through the General Staff Main Directorate for Deep Sea Research (GUGI). One official expressed concern "about heightened Russian naval activity worldwide" and that "Russia's decision calculus for damaging US and allied undersea critical infrastructure may be changing," which could leverage the capabilities mainly being developed through GUGI.[35] The GUGI works independently from Russian naval command and answers directly to the Ministry of Defense, as an intelligence and special mission organization.[36] It operates specialized submarines that can operate in extreme depths (i.e., able to reach undersea cables), surface vessels that collect intelligence, and remotely operated and autonomous underwater vehicles hosted on those surface vessels.[37] For instance, in November 2024, the Russian ship Yantar entered Irish-controlled waters and moved around an area with critical energy pipelines and submarine cables;[38] Yantar is one of the surface fleet ships, with intelligence-gathering capabilities, operated by the GUGI.[39] This is one of several such incidents in recent years, as analysts of the Russian military warn about Moscow's increased emphasis on its submarine fleet.[40]
- Cable Cuts Amid Houthi Red Sea Conflict: As conflict erupted in the Red Sea in March 2024, three submarine cables were cut. There was speculation at first that the Houthi rebels deliberately sabotaged the cables,[41] with the supposed means unspecified, but the White House National Security Council subsequently said that the three cables were likely severed after the Houthis attacked a ship, it started sinking, and its anchor caught the

[34] Rebecca Tan, "Escalating contest over South China Sea disrupts international cable system," *The Washington Post*, October 3, 2024, https://www.washingtonpost.com/world/2024/10/03/south-china-sea-underwater-cables/.
[35] Jim Sciutto, "Exclusive: US sees increasing risk of Russian 'sabotage' of key undersea cables by secretive military unit," CNN, September 6, 2024, https://www.cnn.com/2024/09/06/politics/us-sees-increasing-risk-of-russian-sabotage-undersea-cables/index.html.
[36] Michael Kofman, "Fire aboard AS-31 Losharik: Brief Overview," RussianMilitaryAnalysis.wordpress.com, July 3, 2019, https://russianmilitaryanalysis.wordpress.com/2019/07/03/fire-aboard-as-31-losharik-brief-overview/.
[37] Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," Royal United Services Institute, May 25, 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.
[38] Lisa O'Carroll, "Russian spy ship escorted away from area with critical cables in Irish Sea," *The Guardian*, November 16, 2024, https://www.theguardian.com/world/2024/nov/16/russian-spy-ship-escorted-away-from-internet-cables-in-irish-sea.
[39] Kaushal, "Stalking the Seabed"; H. I. Sutton, "Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables," Naval News, August 19, 2021, https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/.
[40] Andrii Ryzhenko, "Russia Looks to Target Achilles' Heel of Western Economies on Ocean Floor," Jamestown, September 17, 2024, https://web.archive.org/web/20240918081949/https://jamestown.org/program/russia-looks-to-target-achilles-heel-of-western-economies-on-ocean-floor/; Mark Galeotti, "Bear underwater: Russia's undersea capabilities," Council on Geostrategy, June 26, 2023, https://www.geostrategy.org.uk/britains-world/bear-underwater-russias-undersea-capabilities/; Ellie Cook, "NATO Has a Russian Submarine Problem," *Newsweek*, May 13, 2023, https://www.newsweek.com/nato-russia-submarines-nuclear-deterrent-ukraine-arctic-pacific-fleet-kola-peninsula-baltic-1798368.
[41] Jon Gambrell, "3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway," Associated Press, March 4, 2024, https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a.

cables.[42] The incident increased the risk of installing new cables in the Red Sea and especially of ships going out to repair the ones that were severed as the conflict continued.[43]

- Huawei Repairing Subsea Cables: Huawei Marine Networks, part of Chinese telecom Huawei, had by October 2020 built or repaired (by one estimate) roughly 25% of the world's submarine cables.[44] After the Trump administration issued sanctions on Huawei, many companies stopped working with Huawei Marine.[45] In 2020, the UK company Global Marine Group sold its 30% stake in Huawei Marine to the Hengtong Group, China's largest power and fiber optic cable manufacturer.[46] The Hengtong Group then changed Huawei Marine's name to HMN Technologies Co., Ltd., or HMN Tech (ostensibly, HMN as an abbreviation of Huawei Marine Networks),[47] though it has neither helped the brand nor boosted its economic position. Today, Huawei Marine plays a seriously diminished role in submarine cable repairs around the world compared to its market stature just a few years ago.[48]

These are just some examples of the reasons for national security concern. And analyzing the potential threats to the network, whether accidental or intentional, and the available risk mitigations and incident responses are still critical to submarine cable security in any case.

**Zooming In: National Security Risks from China and Russia**

The Chinese government is highly active in the submarine cable arena through a variety of companies. Some of the top Chinese investors in and operators of submarine cables are China Mobile, China Telecom, and China Unicom. For example:

[42] Eleanor Watson, "Ship sunk by Houthis likely responsible for damaging 3 telecommunications cables under Red Sea," CBS News, March 6, 2024, https://www.cbsnews.com/news/houthis-ship-cutting-red-sea-telecommunications-cables/.
[43] Nadine Hawkins, "The underwater digital super highway," CapacityMedia.com, March 11, 2024, https://www.capacitymedia.com/article/2cxmm34wcyeqqxqoo54w0/big-interview/the-underwater-digtal-super-highway; Tim Stronge, "What We Know (And Don't) About Multiple Cable Faults in the Red Sea," TeleGeography, March 5, 2024, https://blog.telegeography.com/what-we-know-and-dont-about-multiple-cable-faults-in-the-red-sea.
[44] U.S. Federal Communications Commission. *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*. FCC-20-133. Washington, D.C.: Federal Communications Commission, October 2020. https://www.fcc.gov/document/fcc-improves-transparency-and-timeliness-foreign-ownership-review. 82.
[45] Anna Gross et al., "How the US is pushing China out of the internet's plumbing," *Financial Times*, June 13, 2023, https://ig.ft.com/subsea-cables/.
[46] Global Marine Group's subsidiary Global Marine Systems Limited established Huawei Marine Networks as a joint venture with Huawei Technology in Tianjin, China, in 2008. Winston Qiu, "Global Marine Group Fully Divests Stake in Huawei Marine Networks," SubmarineNetworks.com, June 6, 2020, https://www.submarinenetworks.com/en/?view=article&id=1334:global-marine-.
[47] HMN Tech, "Huawei Marine Networks Rebrands as HMN Technologies," HMNTech.com, November 3, 2020, https://www.hmntech.com/enPressReleases/37764.jhtml.
[48] Conversations with submarine cable industry experts.

- The Asia Direct Cable (ADC) is expected to be ready for service in Q4 2024. It has landing points in China, Japan, the Philippines, Singapore, Thailand, and Vietnam. Its owners include China Telecom and China Unicom.[49]
- The Asia Pacific Gateway (APG) is active and has landing points in China, Japan, Malaysia, Singapore, South Korea, Taiwan, Thailand, and Vietnam. Its owners include China Mobile, China Telecom, and China Unicom.[50]
- The SeaMeWe-5 is active and has landing points in Bangladesh, Djibouti, Egypt, France, Indonesia, Italy, Malaysia, Myanmar, Oman, Pakistan, Saudi Arabia, Singapore, Sri Lanka, Turkey, the UAE, and Yemen. Its owners include China Mobile, China Telecom, and China Unicom.[51]
- The New Cross Pacific (NCP) cable system is active and has landing points in China, Japan, South Korea, Taiwan, and the United States. Its owners include China Mobile, China Telecom, and China Unicom.[52]

China Mobile, China Telecom, and China Unicom are all state-owned telecommunications companies. They began significantly increasing their investments in submarine cables in 2021.[53] This is a potential national security risk, as they are directly owned by the Chinese government and therefore subject to Chinese government decisions about cable projects—including the possibility of legal and extralegal demands and pressures to assist with government objectives, such as supply chain compromise or espionage. (The FCC, underscoring these risks, denied a China Mobile telecommunication services license application in 2019,[54] revoked China Telecom Americas' Section 214 authority in 2021,[55] revoked China Unicom Americas' telecom services authority in 2022,[56] and added China Telecom Americas and China Mobile to the covered list in 2022.)[57] In fact, many Chinese investors in submarine cables globally are state-owned or state-controlled, widening the same national security risk. For example, these firms include:

[49] "Asia Direct Cable (ADC)," submarinecablemap.com, accessed December 4, 2024, https://www.submarinecablemap.com/submarine-cable/asia-direct-cable-adc.
[50] "Asia Pacific Gateway (APG)," submarinecablemap.com, accessed December 4, 2024, https://www.submarinecablemap.com/submarine-cable/asia-pacific-gateway-apg.
[51] "SeaMeWe-5," submarinecablemap.com, accessed December 4, 2024, https://www.submarinecablemap.com/submarine-cable/seamewe-5.
[52] "New Cross Pacific (NCP) Cable System," submarinecablemap.com, accessed December 6, 2024, https://www.submarinecablemap.com/submarine-cable/new-cross-pacific-ncp-cable-system.
[53] Sherman, *Cyber Defense Across the Ocean Floor*, 13.
[54] U.S. Federal Communications Commission. *FCC Denies China Mobile Telecom Services Application*. FCC-19-38. Washington, D.C.: Federal Communications Commission, May 2019. https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application-0.
[55] U.S. Federal Communications Commission. *China Telecom Americas Order on Revocation and Termination*. FCC-21-114. Washington, D.C.: Federal Communications Commission, November 2021. https://www.fcc.gov/document/china-telecom-americas-order-revocation-and-termination.
[56] U.S. Federal Communications Commission. *China Unicom Americas Order on Revocation*. FCC-22-9. Washington, D.C.: Federal Communications Commission, February 2022. https://www.fcc.gov/document/china-unicom-americas-order-revocation.
[57] U.S. Federal Communications Commission. *Announcement of Additions to the Covered List*. DA-22-320. Washington, D.C.: Federal Communications Commission, March 2022. https://www.fcc.gov/document/announcement-additions-covered-list.

| Entity | Relationship to Chinese Government |
|---|---|
| China Mobile | State-owned |
| China Telecom | State-owned |
| China Unicom | State-owned |
| CITIC Telecom International | State-controlled |
| CTM | State-controlled |

It is additionally possible that the Chinese government legally compels or extralegally coerces a privately owned Chinese company to assist in these activities—though the risk assessment in those scenarios can be complex and depend on a variety of case-specific factors and insights. And it is also possible that organizations that do not appear to be operating out of China, such as certain consortium groups, are in fact subject to Chinese government control. This is not to feed conspiracy theories, but to point out cases such as the National Grid Corporation of the Philippines: nominally, it is only partly owned by a Chinese state-owned electrical company, but CNN reported in 2019 on an internal Filipino government report stating that the Corporation was in fact "under the full control" of the Chinese government and vulnerable to disruption.[58] The National Grid Corporation of the Philippines is the sole owner of an undersea cable connecting two parts of the country—a cable that is also supplied by HMN Tech, previously known as Huawei Marine.[59]

Beyond financing, construction, and management, China's involvement in submarine cable repairs is also a national security concern. Enormous volumes of data traverse submarine cables every day. It is difficult to imagine a scenario in which the Chinese government, with its legal and extralegal ability to coerce technology companies, would not consider placing specific pressure on submarine cable repair companies—or even an individual or individuals at those companies—to assist with tapping into or otherwise compromising that infrastructure for its own advantage.

The US has, in many ways, at least one success story in mitigating this national security risk: the case of Huawei Marine, aka HMN Tech. Huawei Marine went, in just a few years, from repairing or building roughly 25% of the world's subsea cables to a significantly diminished role in the global network. However, Huawei Marine aka HMN Tech does not stand alone. Other Chinese firms such as S.B. Submarine Systems (SBSS) are active in submarine cable repair. SBSS has repaired cables whose owners have included US companies, and its vessels have reportedly, and highly unusually, turned off their transponders at sea and hidden their locations from radio and satellite tracking services, including when traveling and making stops around Singapore, Hong Kong, the Yellow Sea, and even Taiwan.[60] Chinese cable repair ship companies such as SBSS

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

[59] "Sorsogon-Samar Submarine Fiber Optical Interconnection Project (SSSFOIP)," submarinecablemap.com, accessed December 7, 2024, https://www.submarinecablemap.com/submarine-cable/sorsogon-samar-submarine-fiber-optical-interconnection-project-sssfoip.

[60] Dustin Volz et al., "U.S. Fears Undersea Cables Are Vulnerable to Espionage From Chinese Repair Ships," *The Wall Street Journal*, May 19, 2024, https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320. See also a comment in: Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition* (Washington, D.C.: Center for Strategic

present serious national security risks that need to be assessed and considered, including by companies and partners operating in the Asia-Pacific region.

The Russian government, for its part, is not as active as the Chinese government in financing and constructing submarine cables globally. But the Russian government has clearly demonstrated a pattern of thinking about how to physically target and seize control of internet and technological infrastructure to further control over a population (e.g., as it does at home) and to advance its security objectives. Even compared to the views held by the Russian security services in the 1990s and early 2000s, and to the conspiratorialism and concern that cemented in the Kremlin in the late 2000s and early 2010s, the Kremlin has an increasingly paranoid, securitized view of the global internet and of technology.[61] This, coupled with Moscow's aforementioned investments in GUGI, suggests a troubling possibility of Russian government willingness to target submarine cable and other undersea infrastructure for intelligence or military purposes. In that vein, the US intelligence community said in its annual 2024 threat assessment that "Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries."[62] Its annual threat assessment from the year prior noted Russia not just maintains these capabilities but "is particularly focused on improving its ability" to use them, "because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."[63]

It is worth again emphasizing two points, which are not mutually exclusive:

- To avoid threat inflation and ensure an accurate picture of the cable network landscape, it is important for US policymakers and the national security community to recognize the current reality, based on publicly available data, where the majority of damage and disruption to subsea cables is accidental (e.g., a ship dragging an anchor close to a shoreline), as well as caused by natural weather events (e.g., underwater earthquakes), as industry has routinely and repeatedly stressed.
- There are real national security risks facing submarine cables, especially from the Chinese and Russian governments, which may not be accounted for in that data, which often go unconsidered or unprioritized by industry, and which require tailored risk assessment, risk mitigation, and scenario planning—such as for wartime or armed conflict possibilities.

---

and International Studies, August 2024), https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

[61] Justin Sherman, *Russia's Digital Tech Isolation: Domestic Innovation, Digital Fragmentation, and the Kremlin's Push to Replace Western Digital Technology* (Washington, D.C.: Atlantic Council, July 2024), https://dfrlab.org/2024/07/29/russias-digital-tech-isolationism/; Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015).

[62] U.S. Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, D.C.: Office of the Director of National Intelligence, February 2024. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf. 16.

[63] U.S. Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, D.C.: Office of the Director of National Intelligence, February 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf. 15.

**The Vital Role of "Team Telecom"**

When submarine cable companies speak publicly and privately about "security," and conceptualize their own approaches to submarine cable network "security," they are typically speaking about—and thinking about—security in the sense of resilience.[64] This focuses on how submarine cable companies and related organizations, such as governments supporting cable repairs, can ensure cables are quickly and reliably repaired in the event of damage or disruption. And this is an important function, including one performed by the US private sector. Companies may also talk about cybersecurity measures for their systems, such as encryption, and physical access control measures for their facilities, such as fences and cameras around landing stations.

However, this approach to submarine cable "security" fails to capture the wide range of threats posed by foreign actors, including espionage, sabotage, disruption, supply chain infiltration, and the strategic shaping of the global submarine cable network counter to democratic interests. The frequent industry paradigm for subsea cable security also fails to appreciate and factor in the sophistication and persistence of the United States' foreign adversaries, particularly the Chinese and Russian governments, to a degree that far exceeds risks posed by accidental insider behavior and even criminals. Moreover, it does not consider how routine and important functions such as repairing a damaged cable may be difficult already in deep, rough waters, but another scenario entirely when—akin to the Houthi case—rockets or bullets are flying overhead. And this paradigm especially does not account for how a foreign actor may cast typical norms and practices (to the extent norms even exist) out the window in a wartime, armed conflict, or other crisis scenario.

This is precisely why the US government has an executive branch committee, with decades of bipartisan-supported work under its belt, to review submarine cable license applications in the United States and screen them for national security risks. The committee is "Team Telecom."[65] It does not handle every possible risk, such as the risk of a foreign military destroying or damaging a submarine cable in wartime, but it plays an important and necessary role in strategically mitigating national security risks of espionage and supply chain compromise—and in building a base of executive branch expertise about the national security risks facing telecom infrastructure.

In 1995, the Federal Communications Commission (FCC) issued a Report and Order stating that it would consider in foreign carrier applications "any national security, law enforcement, foreign policy, and trade concerns raised by the Executive Branch."[66] The FCC cemented this practice in 1997 with a Report and Order reiterating its interest in soliciting executive branch agencies' views

[64] I have had numerous conversations with submarine cable companies in the United States and around the world about these issues, from technical specialists to executives, as well as other involved organizations.
[65] As I describe in a report for the Hoover Institution, many US government organizations are involved in submarine cable security, though for today's purposes I will focus on Team Telecom's role. See: Justin Sherman, *Cybersecurity Under the Ocean: Submarine Cables and US National Security* (Stanford: Hoover Institution, January 2023), https://www.hoover.org/research/cybersecurity-under-ocean-submarine-cables-and-us-national-security.
[66] U.S. Federal Communications Commission. *Market Entry and Regulation of Foreign-Affiliated Entities*. FCC-95-475. Washington, D.C.: Federal Communications Commission, November 1995. https://www.fcc.gov/document/market-entry-and-regulation-foreign-affiliated-entities-0. 3897.

on national security, law enforcement, foreign policy, and trade considerations[67] vis-à-vis the FCC's Section 214 authority (certificates for foreign carriers),[68] licenses for submarine cable landing stations, and petitions for declaratory rulings under the FCC's Section 310(b) authority (limiting foreign government and certain foreign ownership of telecom licenses).[69] So, for more than 20 subsequent years, the FCC turned to an informal group of executive branch agencies—including the Departments of Defense, Homeland Security, State, and Justice, the US Trade Representative, and the Commerce Department's National Telecommunications & Information Administration (NTIA)—to provide input, including national security input, on its application reviews.[70] This included input on submarine cable license applications as well as proposed assignments or transfers of control of a license for a submarine cable landing.[71]

In 2020, President Trump signed Executive Order 13913 that turned the ad hoc, informal group of agencies advising the FCC into a formal committee.[72] Its new title became the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector—though it still is known by its prior name, Team Telecom. The Department of Justice chairs the committee, through its National Security Division, with committee members from the Department of Defense, Department of Homeland Security, and any other agency or department, or Assistant to the President, that the President designates. The E.O. also specified several committee advisors, from the Secretaries of State, Treasury, and Commerce to the Director of National Intelligence and the President's national security advisor.[73] President Biden kept E.O. 13913 in place when he entered into office, underscoring consensus on this issue set of US telecommunications cybersecurity and resilience, US national security, and foreign adversaries such as Beijing.

From 2013 to 2019, the FCC referred an average of 15% of all international Section 214 and submarine cable applications to Team Telecom for review.[74] Compared to other national security review programs, like the Committee on Foreign Investment in the United States (CFIUS), this program has a relatively narrow, focused purview on a sector of activity with tremendous

---

[67] U.S. Federal Communications Commission. *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*. FCC-97-398. Washington, D.C.: Federal Communications Commission, November 1997. https://www.fcc.gov/document/rules-and-policies-foreign-participation-us-telecommunications. 29.
[68] 47 U.S. Code § 214. https://www.law.cornell.edu/uscode/text/47/214.
[69] 47 U.S. Code § 310. https://www.law.cornell.edu/uscode/text/47/310. See also: U.S. Federal Communications Commission, "Foreign Ownership Rules and Policies for Common Carrier, Aeronautical En Route and Aeronautical Fixed Radio Station Licensees," FCC.gov, accessed December 3, 2024, https://www.fcc.gov/general/foreign-ownership-rules-and-policies-common-carrier-aeronautical-en-route-and-aeronautical.
[70] U.S. Federal Communications Commission. *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*. FCC-20-133. 2-3.
[71] Ibid.
[72] Executive Order 13913. Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector. April 4, 2020. https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states.
[73] The full list of committee advisors as specified in E.O. 13913: the Secretary of State; the Secretary of the Treasury; the Secretary of Commerce; the Director of the Office of Management and Budget; the United States Trade Representative; the Director of National Intelligence; the Administrator of General Services; the Assistant to the President for National Security Affairs; the Assistant to the President for Economic Policy; the Director of the Office of Science and Technology Policy; the Chair of the Council of Economic Advisers; and any other Assistant to the President, as the President determines appropriate.
[74] U.S. Federal Communications Commission. *Process Reform for Executive Branch Review*. FCC-20-133. 5.

implications for US economic and national security—and an area of tremendous interest to actors like the Chinese and Russian governments.

Public Team Telecom actions, and recent demonstrations of its mitigation of potential national security risks, include:

- China Telecom: The FCC's aforementioned, 2021 revocation of China Telecom's Section 214 authority was based on a Team Telecom recommendation, unanimous from the committee's members. Team Telecom found China Telecom to be a national security risk because of the Chinese government's control over China Telecom, the state-owned enterprise's inaccurate public representations of its cybersecurity practices, the nature of China Telecom's US operations, and evolving technological threats from Beijing.[75]
- Pacific Light Cable Network (PLCN): Team Telecom recommended in June 2020 that the FCC refuse to approve cable licensing for the PLCN—a submarine cable involving Google, Facebook, a New Jersey-based telecom, and a Hong Kong-based telecom owned by a Chinese firm—because its routing of US data through Hong Kong allegedly posed a national security risk. One of Team Telecom's specific concerns was that Beijing would compel the Chinese owner of the Hong Kong subsidiary to access data on US persons, and other sensitive data and traffic, traversing the cable. It cited the "current national security environment, including the PRC government's sustained efforts to acquire the sensitive data of millions of US persons" as well as the cable project's "connections to PRC state-owned carrier China Unicom" as reasons for blocking the cable's development.[76] Google and Meta's subsidiaries then withdrew their original FCC application and filed a new one with Hong Kong removed—leaving the landing stations in the United States, Taiwan, and Philippines—which Team Telecom recommended the FCC approve, conditional on the companies' compliance with national security agreements with the committee.[77]
- ARCOS-1 Cable System: Team Telecom recommended in June 2022 that the FCC deny an application by ARCOS-1 USA Inc. and A.Surnet Inc. to modify the ARCOS-1 Cable System—at the time, between the United States, Mexico, Belize, Guatemala, Honduras, Nicaragua, Costa Rica, Panama, Colombia, Venezuela, Curazao, Puerto Rico, the Dominican Republic, Turks and Caicos Islands, and the Bahamas[78]—to add a landing station in Cuba. It cited three factors (non-exhaustive): that Cuba "has long represented a significant counterintelligence threat to the United States," where its direct access to a landing station could be leveraged to further that threat; the risk that traffic not intended

[75] U.S. Department of Justice, "Executive Branch Agencies Recommend the FCC Revoke and Terminate China Telecom's Authorizations to Provide International Telecommunications Services in the United States," Justice.gov, April 9, 2020, https://www.justice.gov/opa/pr/executive-branch-agencies-recommend-fcc-revoke-and-terminate-china-telecom-s-authorizations.

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

[77] U.S. Department of Justice, "Team Telecom Recommends FCC Grant Google and Meta Licenses for Undersea Cable," Justice.gov, December 17, 2021, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable.

[78] "ARCOS," submarinecablemap.com, accessed December 5, 2024, https://www.submarinecablemap.com/submarine-cable/arcos; "ARCOS-1," submarinenetworks.com, accessed December 5, 2024, https://www.submarinenetworks.com/en/systems/brazil-us/arcos-1.

for Cuba could be misrouted by a provider to send the traffic over the cable and to Cuba; and "the Cuban government's relationships with other foreign adversaries, including the People's Republic of China and the Russian Federation," which could enable information-sharing with those governments.[79]

Team Telecom's work has consistently identified national security risks facing the United States through the submarine cable network, particularly vis-à-vis foreign ownership, foreign partnership, landing station, and supply chain risks from the Chinese government, Chinese state-owned telecommunications companies, and other Chinese government-controlled entities. It has also done so in a sector where the traditional industry calculus around "security" and risk does not put US national security at the center—and thinks about "security" in resilience-oriented ways, rather than additionally appreciating the nature of sophisticated foreign threat actors. Team Telecom has also built up a base of expertise within the US government on this problem set and can provide those recommendations to companies, such as through national security agreements, on how to best approach and, if possible, mitigate national security risks that manifest through issues such as company cybersecurity practices, cable network routes, and foreign influence.

The committee's work is also continually evolving. For example, the FCC issued a Notice of Proposed Rulemaking in November 2024, undertaking a major comprehensive review of its submarine cable rules in light of, among others, the "significant" evolution in the national security threat environment in the last two decades.[80] These are welcome and strategically important efforts from the FCC to update national security review processes and regulations to ensure US private-sector companies can keep playing an innovative, competitive role in the global telecommunications system—while simultaneously implementing national security reviews and safeguards to protect against fast-changing threats from foreign governments, especially Beijing and Moscow. Russia's full-on war against Ukraine, concerns about the Chinese government's potential invasion of Taiwan, other escalating security concerns with Beijing's technology activities, and a fast-evolving global threat environment make Team Telecom's work an essential part of identifying and mitigating national security risks in the coming years.

[79] U.S. Department of Justice, "Team Telecom Recommends the FCC Deny Application to Directly Connect the United States to Cuba Through Subsea Cable," Justice.gov, November 30, 2022, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through.

[80] U.S. Federal Communications Commission. *Noticed of Proposed Rulemaking*. FCC-24-119. Washington, D.C.: Federal Communications Commission, November 2024. https://docs.fcc.gov/public/attachments/FCC-24-119A1.pdf.

**Steps Congress Can Take Now**

There are four steps Congress should consider taking now and into the next year.

1. Congress should consider encouraging Team Telecom to continue efforts to increase transparency around the committee and its activities. Team Telecom has been repeatedly criticized over the years for a lack of transparency into its review processes.[81] As I detail in my forthcoming book, there are plenty of reasons for US national security regulations and review programs such as Team Telecom to limit the information shared about their activities, in ways industry sometimes does not recognize—including due to classification issues and the dynamic nature of the geopolitical and cyber threat environment—but it is also important for these review processes to not operate as "black boxes" with opaque criteria that are overly difficult for US companies to navigate. Transparency is important in a democracy. It is important for the US government to be able to simultaneously achieve the objectives of protecting national security and minimizing unnecessary costs to industry. And it is also important for the US government to be able to communicate publicly about risks (such as from Beijing) and earn the trust of private-sector companies, civil society groups, and international partners on these risk mitigations. Team Telecom has made significant progress in increasing the transparency around its processes in the last several years and since President Trump's executive order, including Team Telecom providing public justifications for some of its recent license recommendations and the FCC adopting a set of publicly accessible "Standard Questions" in August 2024[82] that companies must submit in Section 214, submarine cable license, and Section 310(b) filings.[83] These are all important steps. Congress should consider how it can continue to support the committee's efforts at transparency, including by publicly explaining and highlighting the national security risks facing submarine cables, such as from the Chinese government.
2. Congress should consider statutorily authorizing Team Telecom to ensure it has the appropriate authorities, on an ongoing and codified basis, to mitigate national security risks to subsea cables. The statutory authorization of CFIUS in 2007[84] was recognized to be an important moment in cementing the committee's role in screening certain foreign investments in the United States for national security risks. In 2020, a Senate report that reviewed Team Telecom's activities found that the sharing of staff between CFIUS and Team Telecom was counterproductive because some agencies would dual-assign their staffers to both CFIUS and Team Telecom—and the former would receive most of the attention.[85] While they are different review programs with different authorities, scopes, and

[81] See, e.g., U.S. Federal Communications Commission. *Statement of Commissioner Jessica Rosenworcel Re: Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*. Washington, D.C.: Federal Communications Commission, August 2024. https://docs.fcc.gov/public/attachments/FCC-20-133A5.pdf.

[82] U.S. Federal Communications Commission. *Executive Branch Review Rules/Standard Questions Effective August 23, 2024*. Washington, D.C.: Federal Communications Commission, August 2024. https://www.fcc.gov/document/executive-br-review-rulesstandard-questions-effective-aug-23-2024.

[83] See the list of questions: U.S. Federal Communications Commission, "Requirements for Applications and Petitions Subject to Executive Branch Review," FCC.gov, accessed December 4, 2024, https://www.fcc.gov/international-affairs/requirements-applications-and-petitions-subject-executive-branch-review.

[84] This was with the Foreign Investment and National Security Act of 2007 (P.L. 110-49).

[85] U.S. Senate Committee on Homeland Security and Government Affairs: Permanent Subcommittee on Investigations. *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*. Washington, D.C.:

volumes of reviewed transactions and activities, the finding still underscores how statutory authorization from a procedural standpoint can ensure an organization like Team Telecom is effectively staffed. It could ensure it has the authority and Congressional mandate to engage more publicly, including with industry, to the extent possible, on the risks. And it would also be a way to address previously identified, critical national security gaps: Congress could require Team Telecom to periodically reassess foreign carriers, allow Team Telecom to inspect foreign carriers with which it has no existing security agreement, and include a specific requirement for Team Telecom to proactively identify risks associated with changes in ownership throughout the entities involved in the cable supply chain. Congress should consider how statutory authorization of Team Telecom—which could be coupled with an increase in funding and personnel resources—is an appropriate measure to achieve these objectives and continue enabling the committee to confront national security threats, especially from the Chinese and Russian governments.

3. Congress should consider commissioning an open-source study on Chinese government involvement in and risks to the global submarine cable supply chain. There is significant open-source information and data available on the global submarine cable network that can be gathered, coded, and analyzed into a study that is shareable with members of Congress and the public in an open setting. Congress, such as via the Subcommittee, should consider commissioning such a study to give a perspective independent of the submarine cable industry and of the executive branch on the global infrastructure and the national security risks facing the infrastructure; to provide insights of practical use to the Subcommittee and other Members on Chinese government involvement in all aspects of the submarine cable supply chain, including via investments and repairs; to help get a better grasp on Subcommittee and relevant Member-specific questions that are not yet clearly answered; and to better evaluate the national security risks facing subsea cable infrastructure from a geopolitical threat and United States policymaking vantage point. This open-source study could be complemented with public briefings to raise awareness on the issue as well as private briefings for more sensitive open-source findings.
4. Congress should consider requesting a report from the Department of Justice (Team Telecom chair) in conjunction with the Department of Defense on "lessons learned" from Team Telecom in its three decades-long history and since President Trump formalized it into an interagency committee in 2020. Team Telecom has faced significant challenges in its now-decades-long history, ranging from strategic problems (e.g., an insufficient focus on Chinese government activity) to operational roadblocks, due to the nature of Team Telecom's setup (e.g., staff dual-assigned to Team Telecom and programs like CFIUS, the latter of which often ended up receiving more time and attention).[86] Yet, Team Telecom has also, in many ways, made significant progress in tackling these challenges in recent years and since President Trump signed E.O. 13913 in 2020. It has seemingly spent more time focused on threats to submarine cables from the Chinese government, issued more public and plain-language justifications for its recommendations to the FCC on submarine cables, and worked with the FCC to develop new mechanisms to make the program more transparent to industry (e.g., the new Standard Questions). The Senate's bipartisan staff

Senate Committee on Homeland Security and Government Affairs, June 2020. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.

[86] Ibid., 13.

report in 2020 digging into Team Telecom—and, at the time, particularly its failings—was a useful exercise to provide Congress with more information about the committee and to unearth problems and opportunities, but policies and practices have changed. To inform effective oversight, communication to the public about Team Telecom's role and the national security risks to submarine cables, and any future legislative action, Congress should formally request that the Justice Department (as Team Telecom chair), in conjunction with the Defense Department and in consultation with the FCC, author and provide a publicly shareable, unclassified report to Congress on major lessons learned in the design, administration, and threat analysis of its program since the Executive Order in 2020—and describing priority areas and national security risks for the next decade.[87]

The security and resilience of this network are critical to worldwide information flows, commerce, scientific research, military communications, and US national security. Private-sector companies have long played a pivotal role in building and operating this network, and US firms' ability to do so is vital to economic security, national security, and the US' ability to differentiate its internet model from that of Beijing. Simultaneously, foreign actors, particularly the Chinese and Russian governments, pose serious threats to the global submarine cable network and the security of US data flows—making federal government entities like "Team Telecom" essential to protecting our national security, countering Chinese efforts to surveil US subsea cables, and ensuring there is a specialized national security voice in discussions about this global internet infrastructure.

[87] This report could, of course, be accompanied by a non-public annex and/or a classified annex provided solely to the appropriate Members.