Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

CYBER DEFENSE ACROSS THE OCEAN FLOOR

The Geopolitics of Submarine Cable Security

Justin Sherman

Scowcroft Center for Strategy and Security

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

Cyber Statecraft Initiative

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

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

CYBER DEFENSE ACROSS THE OCEAN FLOOR

The Geopolitics of Submarine Cable Security

Justin Sherman

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

Cover: Shutterstock/Vinko93

September 2021

Table of Contents

Executive Summary

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

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

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

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

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

Introduction

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

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

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

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

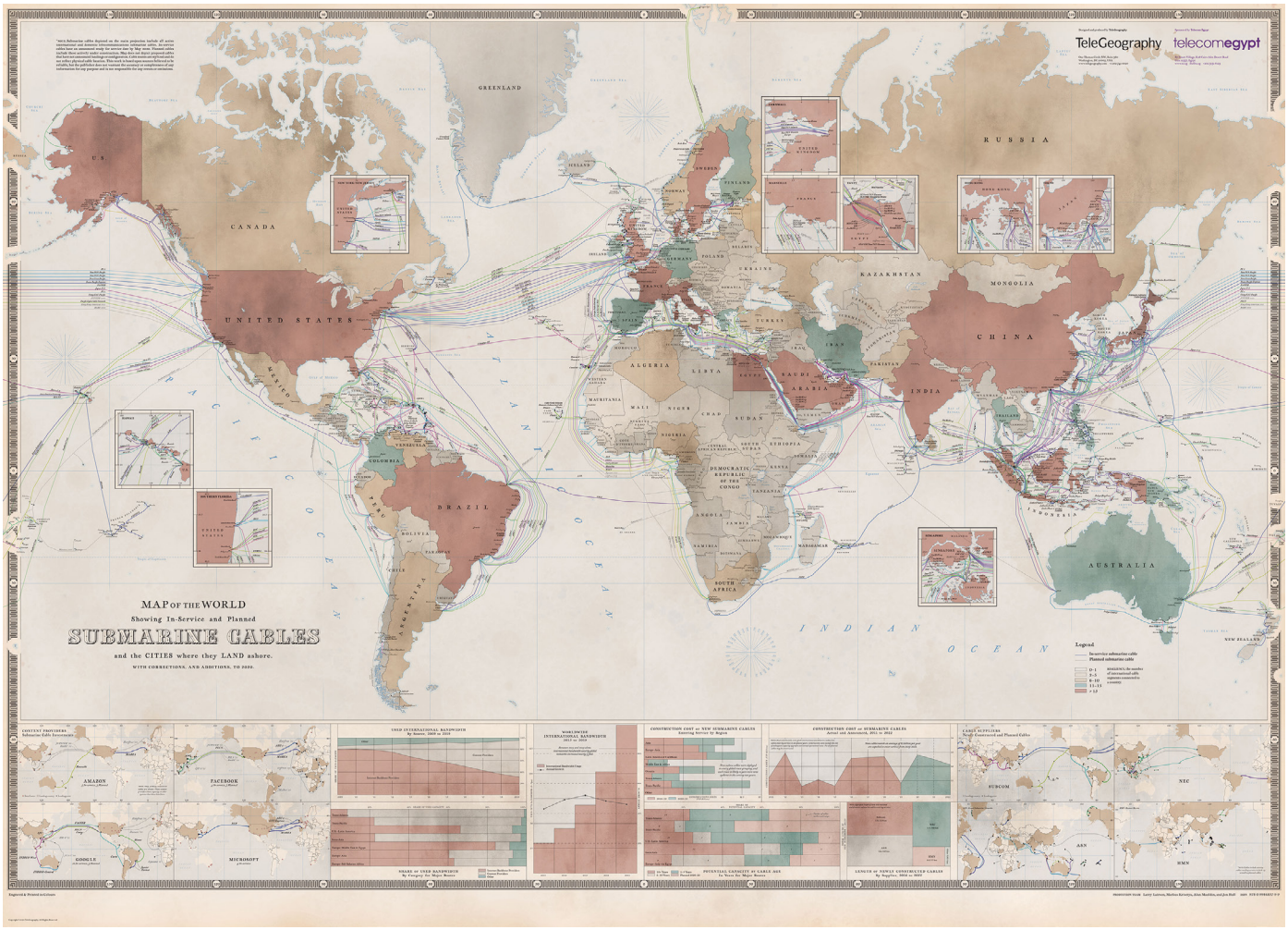
As the White House increasingly focuses on cybersecurity threats to the nation and the global community, including from the Chinese and Russian governments, it must prioritize investing in the security and resilience of the physical infrastructure that underpins Internet communications. US technology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

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

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

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

Image 1: TeleGeography 2020 Submarine Cable Map



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

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

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

Primer: Undersea Cable Development Today

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

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

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

Image 2: Undersea Cable Illustration

Source: iStock

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

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

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

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

History of Undersea Cables

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

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

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

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

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

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

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

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

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

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

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

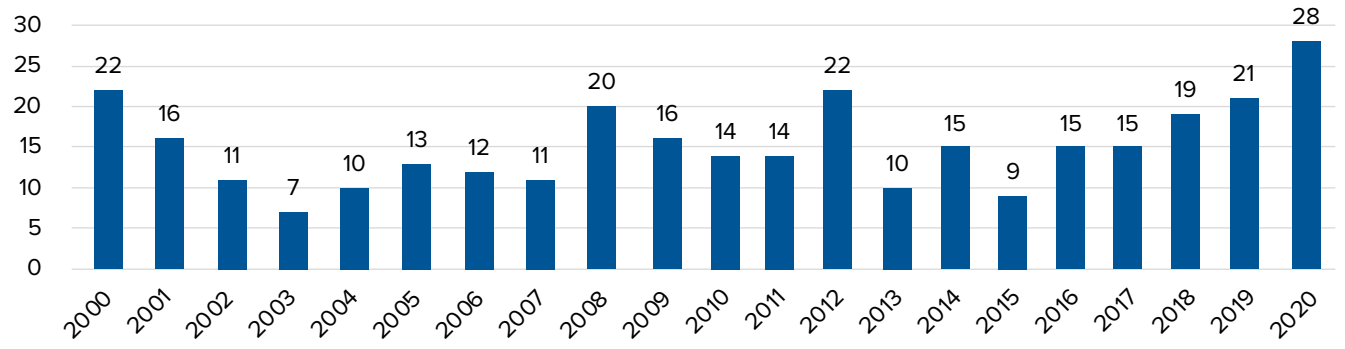
13 For more on this, see Sherman, *The Politics of Internet Security*; Robert Morgus and Justin Sherman, The Idealized Internet vs. Internet Realities (Version 1.0), New America, last updated July 26, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/.

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

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

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

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



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

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

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

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

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

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

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

19 Most damage is caused by natural disasters and accidents.

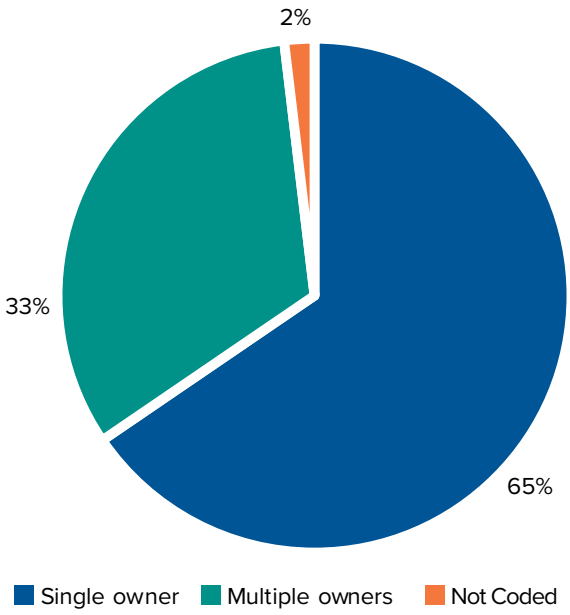
20 Data on the 475 undersea cables deployed worldwide were pulled from the publicly accessible TeleGeography Submarine Cable Map (https://www.submarinecablemap.com/) as of December 2020. Data on the 383 entities that collectively have listed ownership stake in those cables were also pulled from the Submarine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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

Trend 1: Authoritarian Governments Reshaping the Internet through Companies

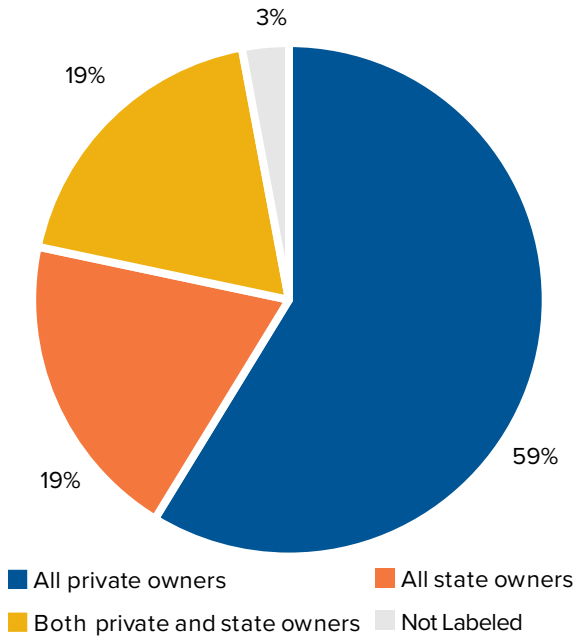
Authoritarian governments are increasingly reshaping the Internet's physical topology (structure) and digital behavior by exerting control over companies. This accelerates security and resilience risks to undersea cables because authoritarian governments—particularly in Beijing and Moscow—can use that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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Source: Visualized by author.

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

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

Risk 1: Chinese State Influence through Cable Owner

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

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

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

38 Sherman, The Politics of Internet Security.

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

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

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

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

Source: TeleGeography's Submarine Cable Map.

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

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

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

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

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

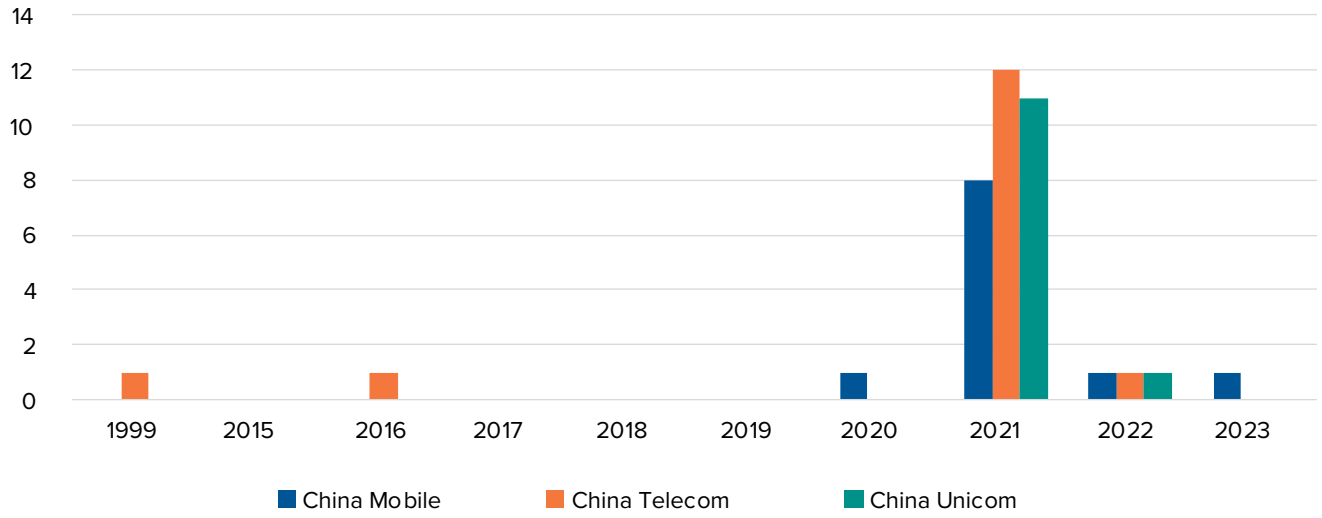
41 U.S. Department of Justice Office of Public Affairs, Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States, press release number 20-555, June 17, 2020, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

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

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

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

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



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

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

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

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

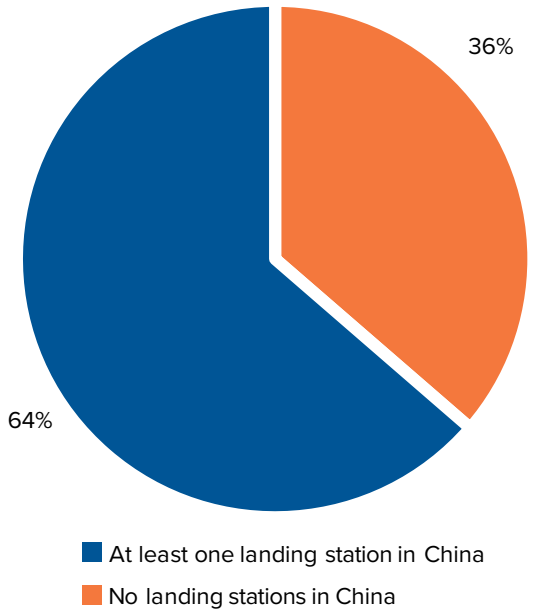
45 US Federal Communications Commission, FCC Denies China Mobile USA Application to Provide Telecommunications Services, press release, May 9, 2019, https://docs.fcc.gov/public/attachments/DOC-357372A1.pdf.

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

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

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

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



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

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

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

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

Risk 2: Chinese State Influence through Cable Builder

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recommendation Previews

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

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

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

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

Trend 2: Companies Using Remote Management Systems for Cable Networks

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

71 Ibid.

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

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

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

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

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

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

Physical Threats to Landing Stations

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

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

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

Recommendation Previews

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

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

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

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

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

82 Ibid., 14.

83 Ibid., 13.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

95 Sherman and Zuo, *Cloud Computing*.

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

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

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

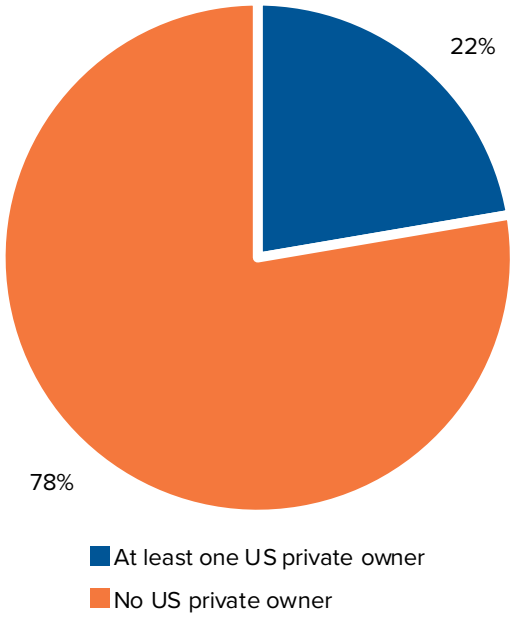
Facebook's investment in submarine cable development is, notably, even more accelerated than that of Amazon or Microsoft. Amazon currently has ownership stake in a 2020 cable and a 2022 cable, and Microsoft has ownership stake in just two 2021 cables, while Facebook has ownership stake in three cables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

Recommendation Previews

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

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

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

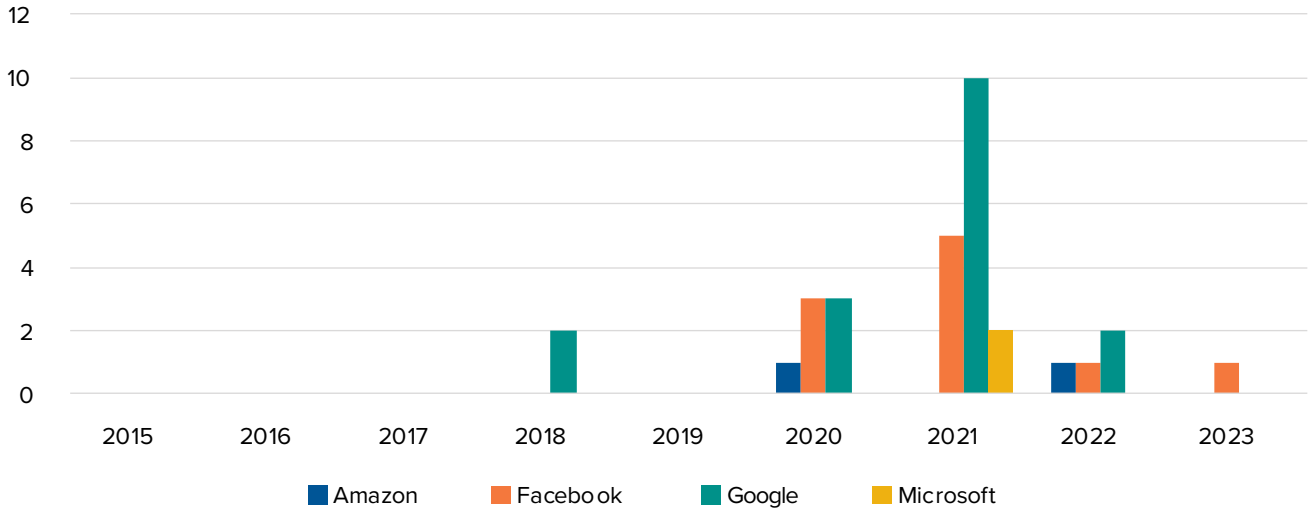


Source: Data from TeleGeography's Submarine Cable Map website visualized by author.

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

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

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



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

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

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

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

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

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

Recommendations

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

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

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

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

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

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

103 Ibid., 43-44.

104 Ibid., 3-4.

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

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

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

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

105 Ibid., 9-10.

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

About the Author

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

Acknowledgments

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

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

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

TREASURER
*George Lund

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

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

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

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

Atlantic Council

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

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